



48-Port 10G Layer 3 Switch

ECS5610-52S

Software Release v1.0.0.0

CLI Reference Guide

CLI Reference Guide

ECS5610-52S

Layer 3 10G Ethernet Switch with
48 10/100/1000BASE-T (RJ-45) Ports,
4 10GBASE SFP+ Ports,
2 Power Supply Units,
and 1 Fan Trays (F2B and B2F Airflow)

How to Use This Guide

This guide includes detailed information on the switch software, including how to operate and use the management functions of the switch. To deploy this switch effectively and ensure trouble-free operation, you should first read the relevant sections in this guide so that you are familiar with all of its software features.

Who Should Read This Guide? This guide is for network administrators who are responsible for operating and maintaining network equipment. The guide assumes a basic working knowledge of LANs (Local Area Networks), the Internet Protocol (IP), and Simple Network Management Protocol (SNMP).

How This Guide is Organized This guide describes the switch's command line interface (CLI). For more detailed information on the switch's key features refer to the *Administrator's Guide*.

The guide includes these sections:

- ◆ Section I **"Getting Started"** — Includes information on connecting to the switch and basic configuration procedures.
- ◆ Section II **"Command Line Interface"** — Includes all management options available through the CLI.
- ◆ Section III **"Appendices"** — Includes information on troubleshooting switch management access.

Related Documentation This guide focuses on switch software configuration through the CLI.

For information on how to manage the switch through the Web management interface, see the following guide:

Web Management Guide



Note: For a general description of switch features, refer to "Introduction" in the *Web Management Guide*.

For information on how to install the switch, see the following guide:

Installation Guide

For all safety information and regulatory statements, see the following documents:

Quick Start Guide
Safety and Regulatory Information

Conventions The following conventions are used throughout this guide to show information:



Note: Emphasizes important information or calls your attention to related features or instructions.



Caution: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.



Warning: Alerts you to a potential hazard that could cause personal injury.

Revision History This section summarizes the changes in each revision of this guide.

August 2013 Revision

This is the first version of this guide. This guide is valid for software release v1.0.0.0.

Contents

How to Use This Guide	3
Contents	5
Figures	43
Tables	45

Section I	Getting Started	53
1	Initial Switch Configuration	55
	Connecting to the Switch	55
	Configuration Options	55
	Connecting to the Console Port	56
	Logging Onto the Command Line Interface	57
	Setting Passwords	57
	Remote Connections (Network Interface or Craft Port)	58
	Configuring the Switch for Remote Management	59
	Using the Service Port or Network Interface	59
	Setting an IP Address	59
	Enabling SNMP Management Access	65
	Managing System Files	67
	Upgrading the Operation Code	68
	Saving or Restoring Configuration Settings	68
	Configuring Automatic Installation of Operation Code and Configuration Settings	70
	Downloading Operation Code from a File Server	70
	Specifying a DHCP Client Identifier	72
	Downloading a Configuration File Referenced by a DHCP Server	73
	Setting the System Clock	75
	Setting the Time Manually	75

Configuring SNTP	76
Configuring NTP	76

Section II	Command Line Interface	79
2	Using the Command Line Interface	81
	Accessing the CLI	81
	Console Connection	81
	Telnet Connection	81
	Entering Commands	83
	Keywords and Arguments	83
	Minimum Abbreviation	83
	Command Completion	83
	Getting Help on Commands	84
	Partial Keyword Lookup	86
	Negating the Effect of Commands	86
	Using Command History	86
	Understanding Command Modes	86
	Exec Commands	87
	Configuration Commands	88
	Command Line Processing	90
	CLI Command Groups	91
3	General Commands	93
	prompt	93
	reload (Global Configuration)	94
	enable	95
	quit	96
	show history	96
	configure	97
	disable	98
	reload (Privileged Exec)	98
	show reload	99
	end	99
	exit	99

4 System Management Commands	101
Device Designation	101
hostname	102
Banner Information	102
banner configure	103
banner configure company	104
banner configure dc-power-info	105
banner configure department	105
banner configure equipment-info	106
banner configure equipment-location	107
banner configure ip-lan	107
banner configure lp-number	108
banner configure manager-info	109
banner configure mux	109
banner configure note	110
show banner	111
System Status	111
location-led	112
show access-list tcam-utilization	112
show location-led status	113
show memory	113
show process cpu	114
show running-config	114
show startup-config	116
show system	116
show tech-support	118
show users	118
show version	119
show watchdog	120
watchdog software	120
Fan Control	121
fan-speed force-full	121
Frame Size	121
jumbo frame	122

File Management	122
General Commands	124
boot system	124
copy	125
delete	128
dir	129
umount usbdisk	130
whichboot	130
Automatic Code Upgrade Commands	131
upgrade opcode auto	131
upgrade opcode path	132
upgrade opcode reload	133
show upgrade	133
Line	134
line	135
databits	135
exec-timeout	136
login	137
parity	138
password	138
password-thresh	139
silent-time	140
speed	141
stopbits	141
timeout login response	142
disconnect	143
terminal	143
show line	144
Event Logging	145
logging facility	145
logging history	146
logging host	147
logging on	147
logging trap	148
clear log	149

show log	149
show logging	150
SMTP Alerts	152
logging sendmail	152
logging sendmail host	152
logging sendmail level	153
logging sendmail destination-email	154
logging sendmail source-email	154
show logging sendmail	155
Time	155
SNTP Commands	156
sntp client	156
sntp poll	157
sntp server	158
show sntp	158
NTP Commands	159
ntp authenticate	159
ntp authentication-key	160
ntp client	161
ntp server	161
show ntp	162
Manual Configuration Commands	163
clock summer-time (date)	163
clock summer-time (predefined)	164
clock summer-time (recurring)	165
clock timezone	167
calendar set	167
show calendar	168
Time Range	169
time-range	169
absolute	170
periodic	171
show time-range	172
Switch Clustering	172
cluster	173

cluster commander	174
cluster ip-pool	174
cluster member	175
rcommand	176
show cluster	176
show cluster members	177
show cluster candidates	177
5 SNMP Commands	179
General SNMP Commands	181
snmp-server	181
snmp-server community	181
snmp-server contact	182
snmp-server location	182
show snmp	183
SNMP Target Host Commands	184
snmp-server enable traps	184
snmp-server host	185
SNMPv3 Commands	187
snmp-server engine-id	187
snmp-server group	188
snmp-server user	189
snmp-server view	191
show snmp engine-id	192
show snmp group	192
show snmp user	194
show snmp view	194
Notification Log Commands	195
nlm	195
snmp-server notify-filter	196
show nlm oper-status	197
show snmp notify-filter	197
Additional Trap Commands	198
memory	198
process cpu	198

6 Remote Monitoring Commands	201
rmon alarm	202
rmon event	203
rmon collection history	204
rmon collection rmon1	205
show rmon alarms	206
show rmon events	206
show rmon history	207
show rmon statistics	207
7 Flow Sampling Commands	209
sflow	209
sflow destination	210
sflow max-datagram-size	211
sflow max-header-size	211
sflow owner	212
sflow polling-interval	212
sflow sample	213
sflow source	213
sflow timeout	214
show sflow	214
8 Authentication Commands	217
User Accounts	218
enable password	218
username	219
Authentication Sequence	220
authentication enable	220
authentication login	221
RADIUS Client	222
radius-server acct-port	222
radius-server auth-port	223
radius-server host	223
radius-server key	224
radius-server retransmit	225
radius-server timeout	225

show radius-server	226
TACACS+ Client	226
tacacs-server host	227
tacacs-server key	227
tacacs-server port	228
tacacs-server retransmit	228
tacacs-server timeout	229
show tacacs-server	229
AAA	230
aaa accounting dot1x	230
aaa accounting exec	231
aaa accounting update	232
aaa authorization exec	233
aaa group server	234
server	234
accounting dot1x	235
accounting exec	235
authorization exec	236
show accounting	236
Web Server	237
ip http port	238
ip http server	238
ip http secure-port	239
ip http secure-server	239
Telnet Server	241
ip telnet max-sessions	241
ip telnet port	242
ip telnet server	242
show ip telnet	243
Secure Shell	243
ip ssh authentication-retries	246
ip ssh server	246
ip ssh server-key size	247
ip ssh timeout	248
delete public-key	248

ip ssh crypto host-key generate	249
ip ssh crypto zeroize	250
ip ssh save host-key	250
show ip ssh	251
show public-key	251
show ssh	252
802.1X Port Authentication	253
General Commands	254
dot1x default	254
dot1x eapol-pass-through	254
dot1x system-auth-control	255
Authenticator Commands	255
dot1x intrusion-action	255
dot1x max-reauth-req	256
dot1x max-req	256
dot1x operation-mode	257
dot1x port-control	258
dot1x re-authentication	258
dot1x timeout quiet-period	259
dot1x timeout re-authperiod	259
dot1x timeout supp-timeout	260
dot1x timeout tx-period	260
dot1x re-authenticate	261
Display Information Commands	261
show dot1x	261
Management IP Filter	264
management	264
show management	265
PPPoE Intermediate Agent	266
pppoe intermediate-agent	267
pppoe intermediate-agent format-type	267
pppoe intermediate-agent port-enable	268
pppoe intermediate-agent port-format-type	269
pppoe intermediate-agent trust	270
pppoe intermediate-agent vendor-tag strip	270

clear pppoe intermediate-agent statistics	271
show pppoe intermediate-agent info	271
show pppoe intermediate-agent statistics	272
9 General Security Measures	275
Port Security	276
mac-learning	276
port security	277
show port security	279
Network Access (MAC Address Authentication)	281
network-access aging	282
network-access mac-filter	282
mac-authentication reauth-time	283
network-access dynamic-qos	284
network-access dynamic-vlan	285
network-access guest-vlan	286
network-access link-detection	286
network-access link-detection link-down	287
network-access link-detection link-up	287
network-access link-detection link-up-down	288
network-access max-mac-count	288
network-access mode mac-authentication	289
network-access port-mac-filter	290
mac-authentication intrusion-action	291
mac-authentication max-mac-count	291
clear network-access	292
show network-access	292
show network-access mac-address-table	293
show network-access mac-filter	294
Web Authentication	294
web-auth login-attempts	295
web-auth quiet-period	296
web-auth session-timeout	296
web-auth system-auth-control	297
web-auth	297

web-auth re-authenticate (Port)	298
web-auth re-authenticate (IP)	298
show web-auth	299
show web-auth interface	299
show web-auth summary	300
DHCPv4 Snooping	300
ip dhcp snooping	301
ip dhcp snooping information option	303
ip dhcp snooping information policy	304
ip dhcp snooping verify mac-address	305
ip dhcp snooping vlan	306
ip dhcp snooping information option circuit-id	307
ip dhcp snooping trust	308
clear ip dhcp snooping binding	309
clear ip dhcp snooping database flash	309
ip dhcp snooping database flash	310
show ip dhcp snooping	310
show ip dhcp snooping binding	311
DHCPv6 Snooping	311
ipv6 dhcp snooping	312
ipv6 dhcp snooping vlan	314
ipv6 dhcp snooping max-binding	315
ipv6 dhcp snooping trust	315
clear ipv6 dhcp snooping binding	317
clear ipv6 dhcp snooping statistics	317
show ipv6 dhcp snooping	318
show ipv6 dhcp snooping binding	318
show ipv6 dhcp snooping statistics	319
IPv4 Source Guard	319
ip source-guard binding	320
ip source-guard	321
ip source-guard max-binding	323
show ip source-guard	323
show ip source-guard binding	324

IPv6 Source Guard	324
ipv6 source-guard binding	325
ipv6 source-guard	326
ipv6 source-guard max-binding	328
show ipv6 source-guard	329
show ipv6 source-guard binding	329
ARP Inspection	330
ip arp inspection	331
ip arp inspection filter	332
ip arp inspection log-buffer logs	333
ip arp inspection validate	334
ip arp inspection vlan	334
ip arp inspection limit	335
ip arp inspection trust	336
show ip arp inspection configuration	337
show ip arp inspection interface	337
show ip arp inspection log	338
show ip arp inspection statistics	338
show ip arp inspection vlan	338
Denial of Service Protection	339
dos-protection land	339
dos-protection tcp-null-scan	340
dos-protection tcp-syn-fin-scan	340
dos-protection tcp-xmas-scan	341
show dos-protection	341
Port-based Traffic Segmentation	342
traffic-segmentation	342
traffic-segmentation session	343
traffic-segmentation uplink/downlink	344
traffic-segmentation uplink-to-uplink	345
show traffic-segmentation	346
10 Access Control Lists	347
IPv4 ACLs	347
access-list ip	348

permit, deny (Standard IP ACL)	349
permit, deny (Extended IPv4 ACL)	350
ip access-group	352
show ip access-group	353
show ip access-list	353
IPv6 ACLs	354
access-list ipv6	354
permit, deny (Standard IPv6 ACL)	355
permit, deny (Extended IPv6 ACL)	356
show ipv6 access-list	357
ipv6 access-group	358
show ipv6 access-group	358
MAC ACLs	359
access-list mac	359
permit, deny (MAC ACL)	360
mac access-group	362
show mac access-group	363
show mac access-list	363
ARP ACLs	364
access-list arp	364
permit, deny (ARP ACL)	365
show arp access-list	366
ACL Information	366
show access-group	366
show access-list	367
11 Interface Commands	369
Interface Configuration	370
interface	370
alias	371
capabilities	372
description	373
flowcontrol	373
history	374
negotiation	375

shutdown	376
switchport block	377
switchport mtu	378
transceiver-threshold-auto	379
transceiver-monitor	379
transceiver-threshold current	380
transceiver-threshold rx-power	381
transceiver-threshold temperature	382
transceiver-threshold tx-power	383
transceiver-threshold voltage	384
clear counters	385
show interfaces brief	385
show interfaces counters	386
show interfaces history	390
show interfaces status	393
show interfaces switchport	394
show interfaces transceiver	396
show interfaces transceiver-threshold	397
Cable Diagnostics	398
test loop internal	398
show loop internal	398
12 Link Aggregation Commands	401
Manual Configuration Commands	402
port channel load-balance	402
channel-group	404
Dynamic Configuration Commands	404
lacp	404
lacp admin-key (Ethernet Interface)	406
lacp port-priority	406
lacp system-priority	407
lacp admin-key (Port Channel)	408
lacp timeout	409
Trunk Status Display Commands	410
show lacp	410

show port-channel load-balance	413
13 Port Mirroring Commands	415
Local Port Mirroring Commands	415
port monitor	415
show port monitor	416
RSPAN Mirroring Commands	417
rspan source	419
rspan destination	420
rspan remote vlan	421
no rspan session	422
show rspan	422
14 Congestion Control Commands	425
Rate Limit Commands	425
rate-limit	426
Storm Control Commands	427
switchport packet-rate	427
Automatic Traffic Control Commands	428
Threshold Commands	431
auto-traffic-control apply-timer	431
auto-traffic-control release-timer	432
auto-traffic-control	433
auto-traffic-control action	433
auto-traffic-control alarm-clear-threshold	434
auto-traffic-control alarm-fire-threshold	435
auto-traffic-control auto-control-release	436
auto-traffic-control control-release	437
SNMP Trap Commands	437
snmp-server enable port-traps atc broadcast-alarm-clear	437
snmp-server enable port-traps atc broadcast-alarm-fire	438
snmp-server enable port-traps atc broadcast-control-apply	438
snmp-server enable port-traps atc broadcast-control-release	439
snmp-server enable port-traps atc multicast-alarm-clear	439
snmp-server enable port-traps atc multicast-alarm-fire	440
snmp-server enable port-traps atc multicast-control-apply	440

snmp-server enable port-traps atc multicast-control-release	441
ATC Display Commands	441
show auto-traffic-control	441
show auto-traffic-control interface	442
15 Address Table Commands	443
mac-address-table aging-time	443
mac-address-table static	444
clear mac-address-table dynamic	445
show mac-address-table	445
show mac-address-table aging-time	446
show mac-address-table count	447
16 Spanning Tree Commands	449
spanning-tree	450
spanning-tree forward-time	451
spanning-tree hello-time	452
spanning-tree max-age	452
spanning-tree mode	453
spanning-tree pathcost method	454
spanning-tree priority	455
spanning-tree mst configuration	456
spanning-tree system-bpdu-flooding	456
spanning-tree transmission-limit	457
max-hops	457
mst priority	458
mst vlan	459
name	460
revision	460
spanning-tree bpdu-filter	461
spanning-tree bpdu-guard	462
spanning-tree cost	463
spanning-tree edge-port	464
spanning-tree link-type	465
spanning-tree loopback-detection	466
spanning-tree loopback-detection action	466

spanning-tree loopback-detection release-mode	467
spanning-tree loopback-detection trap	468
spanning-tree mst cost	468
spanning-tree mst port-priority	469
spanning-tree port-bpdu-flooding	470
spanning-tree port-priority	471
spanning-tree root-guard	471
spanning-tree spanning-disabled	472
spanning-tree loopback-detection release	473
spanning-tree protocol-migration	473
show spanning-tree	474
show spanning-tree mst configuration	476
17 VLAN Commands	477
GVRP and Bridge Extension Commands	478
bridge-ext gvrp	478
garp timer	479
switchport forbidden vlan	480
switchport gvrp	480
show bridge-ext	481
show garp timer	482
show gvrp configuration	483
Editing VLAN Groups	484
vlan database	484
vlan	485
Configuring VLAN Interfaces	486
interface vlan	486
switchport acceptable-frame-types	487
switchport allowed vlan	488
switchport ingress-filtering	489
switchport mode	489
switchport native vlan	490
vlan-trunking	491
Displaying VLAN Information	492
show vlan	492

Configuring IEEE 802.1Q Tunneling	493
dot1q-tunnel system-tunnel-control	494
switchport dot1q-tunnel mode	495
switchport dot1q-tunnel service match cvid	496
switchport dot1q-tunnel tpid	498
show dot1q-tunnel	499
Configuring L2CP Tunneling	500
l2protocol-tunnel tunnel-dmac	500
switchport l2protocol-tunnel	503
show l2protocol-tunnel	504
Configuring VLAN Translation	504
switchport vlan-translation	504
show vlan-translation	506
Configuring Private VLANs	506
private-vlan	508
private vlan association	509
switchport mode private-vlan	509
switchport private-vlan host-association	510
switchport private-vlan mapping	511
show vlan private-vlan	511
Configuring Protocol-based VLANs	512
protocol-vlan protocol-group (Configuring Groups)	513
protocol-vlan protocol-group (Configuring Interfaces)	513
show protocol-vlan protocol-group	514
show interfaces protocol-vlan protocol-group	515
Configuring IP Subnet VLANs	516
subnet-vlan	516
show subnet-vlan	517
Configuring MAC Based VLANs	518
mac-vlan	518
show mac-vlan	519
Configuring Voice VLANs	519
voice vlan	520
voice vlan aging	521
voice vlan mac-address	522

switchport voice vlan	523
switchport voice vlan priority	523
switchport voice vlan rule	524
switchport voice vlan security	525
show voice vlan	525
18 Class of Service Commands	527
Priority Commands (Layer 2)	527
queue mode	528
queue weight	529
switchport priority default	530
show queue mode	531
show queue weight	531
Priority Commands (Layer 3 and 4)	532
qos map phb-queue	533
qos map cos-dscp	534
qos map default-drop-precedence	535
qos map dscp-cos	536
qos map dscp-mutation	537
qos map ip-port-dscp	538
qos map ip-prec-dscp	539
qos map trust-mode	540
show qos map cos-dscp	541
show map default-drop-precedence	541
show map dscp-cos	542
show qos map dscp-mutation	543
show qos map ip-port-dscp	543
show qos map ip-prec-dscp	544
show qos map phb-queue	545
show qos map trust-mode	545
19 Quality of Service Commands	547
class-map	548
description	549
match	549
rename	551

policy-map	551
class	552
police flow	553
police srtcm-color	554
police trtcm-color	557
set cos	559
set phb	560
service-policy	561
show class-map	561
show policy-map	562
show policy-map interface	563
20 Data Center Bridging Commands	565
DCB Exchange Commands	565
dcbx	566
dcbx mode	566
show dcbx	568
Priority-based Flow Control Commands	569
pfc mode	570
pfc priority	571
clear pfc statistics	571
show pfc	572
show pfc statistics	573
Enhanced Transmission Selection Commands	573
ets mode	574
traffic-class algo	575
traffic-class map	576
traffic-class weight	577
show ets mapping	578
show ets weight	579
Congestion Notification Commands	579
cn	582
cn cnm-transmit-priority	582
cn cnpv	583
cn cnpv alternate-priority (Global Configuration)	584

cn cnpv defense-mode (Global Configuration)	585
cn cnpv alternate-priority (Interface Configuration)	586
cn cnpv defense-mode (Interface Configuration)	587
show cn	587
show cn cnpv	588
show cn cp	589
21 Multicast Filtering Commands	591
IGMP Snooping	592
ip igmp snooping	593
ip igmp snooping proxy-reporting	594
ip igmp snooping querier	594
ip igmp snooping router-alert-option-check	595
ip igmp snooping router-port-expire-time	596
ip igmp snooping tcn-flood	596
ip igmp snooping tcn-query-solicit	597
ip igmp snooping unregistered-data-flood	598
ip igmp snooping unsolicited-report-interval	599
ip igmp snooping version	599
ip igmp snooping version-exclusive	600
ip igmp snooping vlan general-query-suppression	601
ip igmp snooping vlan immediate-leave	601
ip igmp snooping vlan last-memb-query-count	602
ip igmp snooping vlan last-memb-query-intvl	603
ip igmp snooping vlan mrd	603
ip igmp snooping vlan proxy-address	604
ip igmp snooping vlan query-interval	606
ip igmp snooping vlan query-resp-intvl	606
ip igmp snooping vlan static	607
clear ip igmp snooping groups dynamic	608
clear ip igmp snooping statistics	608
show ip igmp snooping	608
show ip igmp snooping group	609
show ip igmp snooping mrouter	610
show ip igmp snooping statistics	611

Static Multicast Routing	613
ip igmp snooping vlan mrouter	613
IGMP Filtering and Throttling	614
ip igmp filter (Global Configuration)	615
ip igmp profile	616
permit, deny	616
range	617
ip igmp filter (Interface Configuration)	617
ip igmp max-groups	618
ip igmp max-groups action	619
ip igmp query-drop	619
ip multicast-data-drop	620
show ip igmp filter	620
show ip igmp profile	621
show ip igmp query-drop	622
show ip igmp throttle interface	622
show ip multicast-data-drop	623
MLD Snooping	624
ipv6 mld snooping	625
ipv6 mld snooping querier	625
ipv6 mld snooping query-interval	626
ipv6 mld snooping query-max-response-time	626
ipv6 mld snooping robustness	627
ipv6 mld snooping router-port-expire-time	627
ipv6 mld snooping unknown-multicast mode	628
ipv6 mld snooping version	629
ipv6 mld snooping vlan mrouter	629
ipv6 mld snooping vlan static	630
ipv6 mld snooping vlan immediate-leave	630
show ipv6 mld snooping	631
show ipv6 mld snooping group	632
show ipv6 mld snooping group source-list	632
show ipv6 mld snooping mrouter	633
MVR for IPv4	633
mvr	635

mvr associated-profile	635
mvr domain	636
mvr profile	636
mvr proxy-query-interval	637
mvr proxy-switching	638
mvr robustness-value	639
mvr source-port-mode dynamic	640
mvr upstream-source-ip	640
mvr vlan	641
mvr immediate-leave	642
mvr type	643
mvr vlan group	644
clear mvr groups dynamic	645
clear mvr statistics	645
show mvr	646
show mvr associated-profile	647
show mvr interface	647
show mvr members	648
show mvr profile	650
show mvr statistics	650
MVR for IPv6	653
mvr6 associated-profile	654
mvr6 domain	654
mvr6 profile	655
mvr6 proxy-query-interval	656
mvr6 proxy-switching	657
mvr6 robustness-value	658
mvr6 source-port-mode dynamic	659
mvr6 upstream-source-ip	660
mvr6 vlan	660
mvr6 immediate-leave	661
mvr6 type	662
mvr6 vlan group	663
clear mvr6 groups dynamic	664
clear mvr6 statistics	664

show mvr6	665
show mvr6 associated-profile	666
show mvr6 interface	666
show mvr6 members	667
show mvr6 profile	669
show mvr6 statistics	669
IGMP (Layer 3)	671
ip igmp	672
ip igmp last-member-query-interval	673
ip igmp max-resp-interval	673
ip igmp query-interval	674
ip igmp robustval	675
ip igmp static-group	676
ip igmp version	677
clear ip igmp group	677
show ip igmp groups	678
show ip igmp interface	680
IGMP Proxy Routing	681
ip igmp proxy	681
ip igmp proxy unsolicited-report-interval	683
MLD (Layer 3)	683
ipv6 mld	684
ipv6 mld last-member-query-response-interval	684
ipv6 mld max-resp-interval	685
ipv6 mld query-interval	686
ipv6 mld robustval	687
ipv6 mld static-group	687
ipv6 mld version	688
clear ipv6 mld group	689
show ipv6 mld groups	690
show ipv6 mld interface	691
MLD Proxy Routing	692
ipv6 mld proxy	692
ipv6 mld proxy unsolicited-report-interval	694

22 LLDP Commands	695
lldp	697
lldp holdtime-multiplier	697
lldp med-fast-start-count	698
lldp notification-interval	698
lldp refresh-interval	699
lldp reinit-delay	700
lldp tx-delay	700
lldp admin-status	701
lldp basic-tlv management-ip-address	701
lldp basic-tlv port-description	702
lldp basic-tlv system-capabilities	703
lldp basic-tlv system-description	703
lldp basic-tlv system-name	704
lldp dcbx-tlv ets-config	704
lldp dcbx-tlv ets-recommend	705
lldp dcbx-tlv pfc-config	706
lldp dot1-tlv proto-ident	706
lldp dot1-tlv proto-vid	707
lldp dot1-tlv pvid	707
lldp dot1-tlv vlan-name	708
lldp dot3-tlv link-agg	708
lldp dot3-tlv mac-phy	709
lldp dot3-tlv max-frame	709
lldp med-location civic-addr	710
lldp med-notification	711
lldp med-tlv inventory	712
lldp med-tlv location	713
lldp med-tlv med-cap	713
lldp med-tlv network-policy	714
lldp notification	714
show lldp config	715
show lldp info local-device	716
show lldp info remote-device	717

show lldp info statistics	719
23 Domain Name Service Commands	721
ip domain-list	721
ip domain-lookup	722
ip domain-name	723
ip host	724
ip name-server	724
ipv6 host	725
clear dns cache	726
clear host	726
show dns	727
show dns cache	727
show hosts	728
24 DHCP Commands	729
DHCP Client	729
ip dhcp client class-id	729
ip dhcp restart client	731
ipv6 dhcp client rapid-commit vlan	732
DHCP Relay	733
DHCP for IPv4	733
ip dhcp relay server	733
ip dhcp restart relay	734
DHCP for IPv6	735
ipv6 dhcp relay destination	735
show ipv6 dhcp relay destination	736
DHCP Server	736
ip dhcp excluded-address	737
ip dhcp pool	738
service dhcp	738
bootfile	739
client-identifier	739
default-router	740
dns-server	741
domain-name	741

hardware-address	742
host	743
lease	744
netbios-name-server	744
netbios-node-type	745
network	746
next-server	747
clear ip dhcp binding	747
show ip dhcp binding	748
show ip dhcp	748
25 IP Interface Commands	749
IPv4 Interface	749
Basic IPv4 Configuration	750
ip address	750
ip default-gateway	752
show ip interface	752
show ip traffic	753
traceroute	754
ping	755
ARP Configuration	756
arp	757
arp timeout	758
ip proxy-arp	758
clear arp-cache	759
show arp	759
UDP Helper Configuration	760
ip forward-protocol udp	760
ip helper	761
ip helper-address	762
show ip helper	763
IPv6 Interface	764
Interface Address Configuration and Utilities	765
ipv6 default-gateway	765
ipv6 address	766

ipv6 address eui-64	767
ipv6 address link-local	769
ipv6 enable	770
ipv6 mtu	772
show ipv6 interface	773
show ipv6 mtu	775
show ipv6 traffic	775
clear ipv6 traffic	780
ping6	780
traceroute6	781
Neighbor Discovery	783
ipv6 hop-limit	783
ipv6 nd dad attempts	783
ipv6 nd ns-interval	785
ipv6 nd raguard	786
ipv6 nd reachable-time	787
ipv6 neighbor	788
clear ipv6 neighbors	789
show ipv6 nd raguard	789
show ipv6 neighbors	790
IPv6 to IPv4 Tunnels	791
interface tunnel	793
tunnel destination	793
tunnel mode ipv6ip	795
tunnel source vlan	797
tunnel ttl	797
show ipv6 tunnel	798
26 VRRP Commands	801
vrrp authentication	802
vrrp ip	802
vrrp preempt	803
vrrp priority	804
vrrp timers advertise	805
clear vrrp interface counters	806

clear vrrp router counters	806
show vrrp	806
show vrrp interface	808
show vrrp interface counters	809
show vrrp router counters	810
27 IP Routing Commands	811
Global Routing Configuration	811
IPv4 Commands	812
ip route	812
maximum-paths	813
show ip host-route	813
show ip route	814
show ip route database	815
show ip route summary	816
show ip traffic	816
IPv6 Commands	817
ipv6 route	817
show ipv6 route	819
Routing Information Protocol (RIP)	821
router rip	822
default-information originate	822
default-metric	823
distance	824
maximum-prefix	825
neighbor	825
network	826
passive-interface	827
redistribute	827
timers basic	829
version	830
ip rip authentication mode	831
ip rip authentication string	832
ip rip receive version	832
ip rip receive-packet	833

ip rip send version	834
ip rip send-packet	835
ip rip split-horizon	836
clear ip rip route	836
show ip protocols rip	837
show ip rip	838
Open Shortest Path First (OSPFv2)	839
General Configuration	840
router ospf	840
compatible rfc1583	841
default-information originate	842
router-id	843
timers spf	844
clear ip ospf process	845
Route Metrics and Summaries	845
area default-cost	845
area range	846
auto-cost reference-bandwidth	847
default-metric	848
redistribute	848
summary-address	850
Area Configuration	851
area nssa	851
area stub	852
area virtual-link	854
network area	856
Interface Configuration	857
ip ospf authentication	857
ip ospf authentication-key	859
ip ospf cost	860
ip ospf dead-interval	861
ip ospf hello-interval	861
ip ospf message-digest-key	862
ip ospf priority	863
ip ospf retransmit-interval	864

ip ospf transmit-delay	865
passive-interface	866
Display Information	866
show ip ospf	866
show ip ospf border-routers	868
show ip ospf database	869
show ip ospf interface	875
show ip ospf neighbor	877
show ip ospf route	878
show ip ospf virtual-links	878
show ip protocols ospf	879
Open Shortest Path First (OSPFv3)	880
General Configuration	882
router ipv6 ospf	882
abr-type	883
max-current-dd	884
router-id	885
timers spf	886
Route Metrics and Summaries	886
area default-cost	886
area range	887
default-metric	888
redistribute	889
Area Configuration	890
area stub	890
area virtual-link	891
ipv6 router ospf area	893
ipv6 router ospf tag area	894
Interface Configuration	895
ipv6 ospf cost	895
ipv6 ospf dead-interval	896
ipv6 ospf hello-interval	897
ipv6 ospf priority	897
ipv6 ospf retransmit-interval	898
ipv6 ospf transmit-delay	899

passive-interface	900
Display Information	900
show ipv6 ospf	900
show ipv6 ospf database	902
show ipv6 ospf interface	903
show ipv6 ospf neighbor	904
show ipv6 ospf route	905
show ipv6 ospf virtual-links	906
Border Gateway Protocol (BGPv4)	907
BGP Overview	907
External and Internal BGP	907
BGP Routing Basics	909
Internal BGP Scalability	912
Route Flap Dampening	916
BGP Command List	917
General Configuration	921
router bgp	921
ip as-path access-list	922
ip community-list	923
ip extcommunity-list	925
ip prefix-list	927
aggregate-address	928
bgp client-to-client reflection	930
bgp cluster-id	931
bgp confederation identifier	932
bgp confederation peer	933
bgp dampening	934
bgp enforce-first-as	935
bgp fast-external-failover	935
bgp log-neighbor-changes	936
bgp network import-check	936
bgp router-id	937
bgp scan-time	937
network	938
redistribute	939

timers bgp	940
clear ip bgp	941
clear ip bgp dampening	942
Route Metrics and Selection	943
bgp always-compare-med	943
bgp bestpath as-path ignore	944
bgp bestpath compare-confed-aspath	944
bgp bestpath compare-routerid	944
bgp bestpath med	945
bgp default local-preference	946
bgp deterministic-med	946
distance	947
distance bgp	948
Neighbor Configuration	949
neighbor activate	949
neighbor advertisement-interval	950
neighbor allowas-in	950
neighbor attribute-unchanged	951
neighbor capability dynamic	952
neighbor capability orf prefix-list	952
neighbor default-originate	953
neighbor description	954
neighbor distribute-list	954
neighbor dont-capability-negotiate	955
neighbor ebgp-multihop	956
neighbor enforce-multihop	957
neighbor filter-list	957
neighbor interface	958
neighbor maximum-prefix	959
neighbor next-hop-self	960
neighbor override-capability	960
neighbor passive	961
neighbor peer-group (Creating)	961
neighbor peer-group (Group Members)	962
neighbor port	963

neighbor prefix-list	963
neighbor remote-as	964
neighbor remove-private-as	965
neighbor route-map	966
neighbor route-reflector-client	966
neighbor route-server-client	967
neighbor send-community	968
neighbor shutdown	969
neighbor soft-reconfiguration inbound	969
neighbor strict-capability-match	970
neighbor timers	971
neighbor timers connect	972
neighbor unsuppress-map	972
neighbor update-source	973
neighbor weight	974
Display Information	974
show ip bgp	974
show ip bgp attribute-info	976
show ip bgp cidr-only	976
show ip bgp community	977
show ip bgp community-info	978
show ip bgp community-list	978
show ip bgp dampening	979
show ip bgp filter-list	980
show ip bgp neighbors	981
show ip bgp paths	982
show ip bgp prefix-list	983
show ip bgp regexp	983
show ip bgp route-map	984
show ip bgp scan	984
show ip bgp summary	985
show ip community-list	985
show ip extcommunity-list	986
show ip prefix-list	986
show ip prefix-list detail	987

show ip prefix-list summary	987
Policy-based Routing for BGP	988
route-map	990
call	991
continue	992
description	992
match as-path	993
match community	993
match extcommunity	994
match ip address	995
match ip next-hop	995
match ip route-source	996
match metric	996
match origin	997
match pathlimit	997
match peer	998
on-match	999
set aggregator as	999
set as-path	1000
set atomic-aggregate	1001
set comm-list delete	1001
set community	1002
set extcommunity	1003
set ip next-hop	1004
set local-preference	1005
set metric	1006
set origin	1006
set originator-id	1007
set pathlimit ttl	1008
set weight	1008
show route-map	1009
28 Multicast Routing Commands	1011
General Multicast Routing	1011
ip multicast-routing	1011

show ip mroute	1012
ipv6 multicast-routing	1014
show ipv6 mroute	1015
Static Multicast Routing	1017
ip igmp snooping vlan mrouter	1017
show ip igmp snooping mrouter	1018
PIM Multicast Routing	1019
IPv4 PIM Commands	1019
PIM Shared Mode Commands	1020
router pim	1020
ip pim	1021
ip pim hello-holdtime	1022
ip pim hello-interval	1023
ip pim join-prune-holdtime	1023
ip pim lan-prune-delay	1024
ip pim override-interval	1025
ip pim propagation-delay	1026
ip pim trigger-hello-delay	1026
show ip pim interface	1027
show ip pim neighbor	1028
PIM-DM Commands	1028
ip pim graft-retry-interval	1028
ip pim max-graft-retries	1029
ip pim state-refresh origination-interval	1029
PIM-SM Commands	1030
ip pim bsr-candidate	1030
ip pim register-rate-limit	1032
ip pim register-source	1032
ip pim rp-address	1033
ip pim rp-candidate	1035
ip pim spt-threshold	1036
ip pim dr-priority	1037
ip pim join-prune-interval	1038
clear ip pim bsr rp-set	1039
show ip pim bsr-router	1040

show ip pim rp mapping	1041
show ip pim rp-hash	1042
IPv6 PIM Commands	1042
PIM6 Shared Mode Commands	1043
router pim6	1043
ipv6 pim	1044
ipv6 pim hello-holdtime	1045
ipv6 pim hello-interval	1046
ipv6 pim join-prune-holdtime	1046
ipv6 pim lan-prune-delay	1047
ipv6 pim override-interval	1048
ipv6 pim propagation-delay	1049
ipv6 pim trigger-hello-delay	1049
show ipv6 pim interface	1050
show ipv6 pim neighbor	1051
PIM6-DM Commands	1051
ipv6 pim graft-retry-interval	1051
ipv6 pim max-graft-retries	1052
ipv6 pim state-refresh origination-interval	1053
PIM6-SM Commands	1054
ipv6 pim bsr-candidate	1054
ipv6 pim register-rate-limit	1055
ipv6 pim register-source	1056
ipv6 pim rp-address	1056
ipv6 pim rp-candidate	1058
ipv6 pim spt-threshold	1059
ipv6 pim dr-priority	1060
ipv6 pim join-prune-interval	1061
clear ipv6 pim bsr rp-set	1062
show ipv6 pim bsr-router	1063
show ipv6 pim rp mapping	1064
show ipv6 pim rp-hash	1064

Section III	Appendices	1067
	A Troubleshooting	1069
	Problems Accessing the Management Interface	1069
	Using System Logs	1070
	B License Information	1071
	The GNU General Public License	1071
	Glossary	1075
	Index of CLI Commands	1083
	Index	1093

Figures

Figure 1: Storm Control by Limiting the Traffic Rate	430
Figure 2: Storm Control by Shutting Down a Port	431
Figure 3: Configuring VLAN Trunking	491
Figure 4: Mapping QinQ Service VLAN to Customer VLAN	497
Figure 5: Configuring VLAN Translation	505
Figure 6: Connections for Internal and External BGP	908
Figure 7: Connections for Single Route Reflector	913
Figure 8: Connections for Multiple Route Reflectors	913
Figure 9: Connections for BGP Confederation	915
Figure 10: Connections for Route Server	916

Tables

Table 1: Options 60, 66 and 67 Statements	74
Table 2: Options 55 and 124 Statements	74
Table 3: General Command Modes	87
Table 4: Configuration Command Modes	89
Table 5: Keystroke Commands	90
Table 6: Command Group Index	91
Table 7: General Commands	93
Table 8: System Management Commands	101
Table 9: Device Designation Commands	101
Table 10: Banner Commands	102
Table 11: System Status Commands	111
Table 12: show system – display description	117
Table 13: show version – display description	120
Table 14: Fan Control Commands	121
Table 15: Frame Size Commands	121
Table 16: Flash/File Commands	123
Table 17: File Directory Information	129
Table 18: Line Commands	134
Table 19: Event Logging Commands	145
Table 20: Logging Levels	146
Table 21: show logging flash/ram - display description	151
Table 22: show logging trap - display description	151
Table 23: Event Logging Commands	152
Table 24: Time Commands	155
Table 25: Predefined Summer-Time Parameters	165
Table 26: Time Range Commands	169
Table 27: Switch Cluster Commands	172
Table 28: SNMP Commands	179
Table 29: show snmp engine-id - display description	192

Table 30: show snmp group - display description	193
Table 31: show snmp user - display description	194
Table 32: show snmp view - display description	195
Table 33: RMON Commands	201
Table 34: sFlow Commands	209
Table 35: Authentication Commands	217
Table 36: User Access Commands	218
Table 37: Default Login Settings	219
Table 38: Authentication Sequence Commands	220
Table 39: RADIUS Client Commands	222
Table 40: TACACS+ Client Commands	226
Table 41: AAA Commands	230
Table 42: Web Server Commands	237
Table 43: HTTPS System Support	240
Table 44: Telnet Server Commands	241
Table 45: Secure Shell Commands	243
Table 46: show ssh - display description	252
Table 47: 802.1X Port Authentication Commands	253
Table 48: Management IP Filter Commands	264
Table 49: PPPoE Intermediate Agent Commands	266
Table 50: show pppoe intermediate-agent statistics - display description	272
Table 51: General Security Commands	275
Table 52: Management IP Filter Commands	276
Table 53: show port security - display description	279
Table 54: Network Access Commands	281
Table 55: Dynamic QoS Profiles	284
Table 56: Web Authentication	295
Table 57: DHCP Snooping Commands	300
Table 58: Option 82 information	307
Table 59: DHCP Snooping Commands	311
Table 60: IPv4 Source Guard Commands	319
Table 61: IPv6 Source Guard Commands	324
Table 62: ARP Inspection Commands	330
Table 63: DoS Protection Commands	339
Table 64: Commands for Configuring Traffic Segmentation	342

Table 65: Traffic Segmentation Forwarding	343
Table 66: Access Control List Commands	347
Table 67: IPv4 ACL Commands	347
Table 68: IPv6 ACL Commands	354
Table 69: MAC ACL Commands	359
Table 70: ARP ACL Commands	364
Table 71: ACL Information Commands	366
Table 72: Interface Commands	369
Table 73: show interfaces counters - display description	387
Table 74: show interfaces switchport - display description	395
Table 75: Link Aggregation Commands	401
Table 76: show lacp counters - display description	410
Table 77: show lacp internal - display description	411
Table 78: show lacp neighbors - display description	412
Table 79: show lacp sysid - display description	413
Table 80: Port Mirroring Commands	415
Table 81: Mirror Port Commands	415
Table 82: RSPAN Commands	417
Table 83: Congestion Control Commands	425
Table 84: Rate Limit Commands	425
Table 85: Rate Limit Commands	427
Table 86: ATC Commands	428
Table 87: Address Table Commands	443
Table 88: Spanning Tree Commands	449
Table 89: Recommended STA Path Cost Range	463
Table 90: Default STA Path Costs	463
Table 91: VLAN Commands	477
Table 92: GVRP and Bridge Extension Commands	478
Table 93: show bridge-ext - display description	481
Table 94: Commands for Editing VLAN Groups	484
Table 95: Commands for Configuring VLAN Interfaces	486
Table 96: Commands for Displaying VLAN Information	492
Table 97: 802.1Q Tunneling Commands	493
Table 98: L2 Protocol Tunnel Commands	500
Table 99: VLAN Translation Commands	504

Table 100: Private VLAN Commands	507
Table 101: Protocol-based VLAN Commands	512
Table 102: IP Subnet VLAN Commands	516
Table 103: MAC Based VLAN Commands	518
Table 104: Voice VLAN Commands	519
Table 105: Priority Commands	527
Table 106: Priority Commands (Layer 2)	527
Table 107: Priority Commands (Layer 3 and 4)	532
Table 108: Mapping Internal Per-hop Behavior to Hardware Queues	533
Table 109: Default Mapping of CoS/CFI to Internal PHB/Drop Precedence	534
Table 110: Mapping Per-hop Behavior to Drop Precedence	535
Table 111: Mapping Internal PHB/Drop Precedence to CoS/CFI Values	536
Table 112: Default Mapping of DSCP Values to Internal PHB/Drop Values	537
Table 113: Default Mapping of IP Precedence to Internal PHB/Drop Values	539
Table 114: Quality of Service Commands	547
Table 115: Data Center Bridging Commands	565
Table 116: DCB Exchange Commands	565
Table 117: Priority-based Flow Control Commands	569
Table 118: ETS Commands	574
Table 119: CN Commands	581
Table 120: show cn cp - display description	589
Table 121: Multicast Filtering Commands	591
Table 122: IGMP Snooping Commands	592
Table 123: show ip igmp snooping statistics input - display description	612
Table 124: show ip igmp snooping statistics output - display description	612
Table 125: show ip igmp snooping statistics vlan query - display description	613
Table 126: Static Multicast Interface Commands	613
Table 127: IGMP Filtering and Throttling Commands	614
Table 128: MLD Snooping Commands	624
Table 129: Multicast VLAN Registration for IPv4 Commands	633
Table 130: show mvr - display description	646
Table 131: show mvr interface - display description	648
Table 132: show mvr members - display description	650
Table 133: show mvr statistics input - display description	651
Table 134: show mvr statistics output - display description	652

Table 135: show mvr statistics query - display description	652
Table 136: Multicast VLAN Registration for IPv6 Commands	653
Table 137: show mvr6 - display description	665
Table 138: show mvr6 interface - display description	667
Table 139: show mvr6 members - display description	668
Table 140: show mvr6 statistics input - display description	670
Table 141: show mvr6 statistics output - display description	670
Table 142: IGMP Commands (Layer 3)	671
Table 143: show ip igmp groups - display description	679
Table 144: show ip igmp groups detail - display description	679
Table 145: IGMP Proxy Commands	681
Table 146: MLD Commands (Layer 3)	683
Table 147: show ipv6 mld groups - display description	690
Table 148: IGMP Proxy Commands	692
Table 149: LLDP Commands	695
Table 150: LLDP MED Location CA Types	710
Table 151: Address Table Commands	721
Table 152: show dns cache - display description	727
Table 153: show hosts - display description	728
Table 154: DHCP Commands	729
Table 155: DHCP Client Commands	729
Table 156: Options 60, 66 and 67 Statements	730
Table 157: Options 55 and 124 Statements	730
Table 158: DHCP Relay Commands	733
Table 159: DHCP Server Commands	736
Table 160: IP Interface Commands	749
Table 161: IPv4 Interface Commands	749
Table 162: Basic IP Configuration Commands	750
Table 163: Address Resolution Protocol Commands	756
Table 164: UDP Helper Commands	760
Table 165: IPv6 Configuration Commands	764
Table 166: show ipv6 interface - display description	774
Table 167: show ipv6 mtu - display description	775
Table 168: show ipv6 traffic - display description	777
Table 169: show ipv6 neighbors - display description	790

Table 170: IPv6 to IPv4 Tunnelling Commands	791
Table 171: VRRP Commands	801
Table 172: show vrrp - display description	807
Table 173: show vrrp brief - display description	808
Table 174: IP Routing Commands	811
Table 175: Global Routing Configuration Commands	811
Table 176: show ip host-route - display description	814
Table 177: Routing Information Protocol Commands	821
Table 178: Open Shortest Path First Commands	839
Table 179: show ip ospf - display description	867
Table 180: show ip ospf database - display description	870
Table 181: show ip ospf database summary - display description	871
Table 182: show ip ospf database external - display description	872
Table 183: show ip ospf database network - display description	873
Table 184: show ip ospf database router - display description	874
Table 185: show ip ospf database summary - display description	875
Table 186: show ip ospf interface - display description	876
Table 187: show ip ospf neighbor - display description	877
Table 188: show ip ospf virtual-links - display description	879
Table 189: show ip protocols ospf - display description	879
Table 190: Open Shortest Path First Commands (Version 3)	880
Table 191: show ip ospf - display description	901
Table 192: show ip ospf database - display description	903
Table 193: show ip ospf interface - display description	903
Table 194: show ipv6 ospf neighbor - display description	905
Table 195: show ipv6 ospf virtual-links - display description	906
Table 196: Border Gateway Protocol Commands – Version 4	917
Table 197: show ip bgp - display description	975
Table 198: show ip bgp community-info - display description	978
Table 199: show ip bgp dampening parameters- display description	980
Table 200: show ip bgp - display description	982
Table 201: show ip bgp paths - display description	983
Table 202: Policy-based Routing Configuration Commands	988
Table 203: Multicast Routing Commands	1011
Table 204: General Multicast Routing Commands	1011

Table 205: show ip mroute - display description	1013
Table 206: show ip mroute - display description	1016
Table 207: Static Multicast Routing Commands	1017
Table 208: IPv4 and IPv6 PIM Commands	1019
Table 209: PIM-DM and PIM-SM Multicast Routing Commands	1019
Table 210: show ip pim neighbor - display description	1028
Table 211: show ip pim bsr-router - display description	1040
Table 212: show ip pim rp mapping - display description	1041
Table 213: show ip pim rp-hash - display description	1042
Table 214: PIM-DM and PIM-SM Multicast Routing Commands	1042
Table 215: show ipv6 pim neighbor - display description	1051
Table 216: show ip pim bsr-router - display description	1063
Table 217: show ip pim rp mapping - display description	1064
Table 218: show ip pim rp-hash - display description	1065
Table 219: Troubleshooting Chart	1069

Section I

Getting Started

This section provides an overview of the switch, and introduces some basic concepts about network switches. It also describes the basic settings required to access the management interface.

This section includes these chapters:

- ◆ ["Initial Switch Configuration" on page 55](#)

1

Initial Switch Configuration

This chapter includes information on connecting to the switch and basic configuration procedures.

Connecting to the Switch

The switch includes a built-in network management agent. The agent offers a variety of management options, including SNMP, RMON and a web-based interface. A PC may also be connected directly to the switch for configuration and monitoring via a command line interface (CLI).



Note: An IPv4 address for this switch is obtained via DHCP by default. To change this address, see [“Setting an IP Address” on page 59](#).

Configuration Options

The switch’s HTTP web agent allows you to configure switch parameters, monitor port connections, and display statistics using a standard web browser such as Internet Explorer 6 or above, and Mozilla Firefox 4 or above. The switch’s web management interface can be accessed from any computer attached to the network.

The CLI program can be accessed by a direct connection to the RS-232 serial console port on the switch, or remotely by a Telnet connection over the network.

The switch’s management agent also supports SNMP (Simple Network Management Protocol). This SNMP agent permits the switch to be managed from any system in the network using network management software.

The switch’s web interface, console interface, and SNMP agent allow you to perform the following management functions:

- ◆ Set user names and passwords
- ◆ Set an IP interface for a management any VLAN
- ◆ Configure SNMP parameters
- ◆ Enable/disable any port
- ◆ Set the speed/duplex mode for any port
- ◆ Configure the bandwidth of any port by limiting input or output rates

- ◆ Control port access through IEEE 802.1X security or static address filtering
- ◆ Filter packets using Access Control Lists (ACLs)
- ◆ Configure up to 4094 IEEE 802.1Q VLANs
- ◆ Enable GVRP automatic VLAN registration
- ◆ Configure IP routing for unicast or multicast traffic
- ◆ Configure router redundancy
- ◆ Configure IGMP multicast filtering
- ◆ Upload and download system firmware or configuration files via HTTP (using the web interface) or FTP/TFTP (using the command line or web interface)
- ◆ Configure Spanning Tree parameters
- ◆ Configure Class of Service (CoS) priority queuing
- ◆ Configure static or LACP trunks (up to 8)
- ◆ Enable port mirroring
- ◆ Set storm control on any port for excessive broadcast, multicast, or unknown unicast traffic
- ◆ Display system information and statistics

Connecting to the Console Port

The switch provides an RS-232 serial port that enables a connection to a PC or terminal for monitoring and configuring the switch. A null-modem console cable is provided with the switch.

Attach a VT100-compatible terminal, or a PC running a terminal emulation program to the switch. You can use the console cable provided with this package, or use a null-modem cable that complies with the wiring assignments shown in the Installation Guide.

To connect a terminal to the console port, complete the following steps:

- 1.** Connect the console cable to the serial port on a terminal, or a PC running terminal emulation software, and tighten the captive retaining screws on the DB-9 connector.
- 2.** Connect the other end of the cable to the RS-45 serial port on the switch.
- 3.** Make sure the terminal emulation software is set as follows:
 - Select the appropriate serial port (COM port 1 or COM port 2).
 - Set the baud rate to 115200 bps.
 - Set the data format to 8 data bits, 1 stop bit, and no parity.
 - Set flow control to none.
 - Set the emulation mode to VT100.

- When using HyperTerminal, select Terminal keys, not Windows keys.

4. Power on the switch.

After the system completes the boot cycle, the logon screen appears.

**Logging Onto the
Command Line
Interface**

The CLI program provides two different command levels — normal access level (Normal Exec) and privileged access level (Privileged Exec). The commands available at the Normal Exec level are a limited subset of those available at the Privileged Exec level and allow you to only display information and use basic utilities. To fully configure the switch parameters, you must access the CLI at the Privileged Exec level.

Access to both CLI levels are controlled by user names and passwords. The switch has a default user name and password for each level. To log into the CLI at the Privileged Exec level using the default user name and password, perform these steps:

1. To initiate your console connection, press <Enter>. The “User Access Verification” procedure starts.
2. At the User Name prompt, enter “admin.”
3. At the Password prompt, also enter “admin.” (The password characters are not displayed on the console screen.)
4. The session is opened and the CLI displays the “Console#” prompt indicating you have access at the Privileged Exec level.

Setting Passwords

If this is your first time to log into the CLI program, you should define new passwords for both default user names using the “username” command, record them and put them in a safe place.

Passwords can consist of up to 32 alphanumeric characters and are case sensitive. To prevent unauthorized access to the switch, set the passwords as follows:

1. Open the console interface with the default user name and password “admin” to access the Privileged Exec level.
2. Type “configure” and press <Enter>.
3. Type “username guest password 0 *password*,” for the Normal Exec level, where *password* is your new password. Press <Enter>.
4. Type “username admin password 0 *password*,” for the Privileged Exec level, where *password* is your new password. Press <Enter>.

```
Username: admin
Password:

CLI session with the ECS5610-52S is opened.
To end the CLI session, enter [Exit].

Console#configure
Console(config)#username guest password 0 [password]
Console(config)#username admin password 0 [password]
Console(config)#
```

Remote Connections (Network Interface or Craft Port)

Prior to accessing the switch's onboard agent via a network connection, you must first configure the switch's network interface or craft port with a valid IPv4 or IPv6 address.

The default network interface is VLAN 1 which includes ports 1-52. However, note that the switch also includes a Craft port on the front panel which provides a secure management channel that is isolated from all other ports on the switch. This interface is not configured with an IP address by default, but may be manually configured with an IPv4 or IPv6 address. The Craft port is specified with the name "craft" in the commands used to configure its IP address.

When configuring the network interface, the IP address, subnet mask, and default gateway may all be set using a console connection, or DHCP protocol as described in the following sections.

An IPv4 address for the primary network interface is obtained via DHCP by default. To manually configure this address or enable dynamic address assignment via DHCP, see ["Setting an IP Address" on page 59](#).

After configuring the switch's IP parameters, you can access the onboard configuration program from anywhere within the attached network. The onboard configuration program can be accessed using Telnet or SSH from any computer attached to the network. The switch can also be managed by any computer using a web browser (Internet Explorer 6 or above, and Mozilla Firefox 4 or above).



Note: This switch supports eight Telnet sessions or SSH sessions.

The onboard program only provides access to basic configuration functions. To access the full range of SNMP management functions, you must use SNMP-based network management software.

Configuring the Switch for Remote Management

Using the Service Port or Network Interface The service port is a dedicated for out-of-band management. In general, the service port should be used to manage the switch for security reasons. Traffic on this port is segregated from normal network traffic on other switch ports and cannot be switched or routed to the operational network. Additionally, if the operational network is experiencing problems, the service port still allows you to access the switch's management interface and troubleshoot network problems. Configuration options on the service port are limited, which makes it difficult to accidentally cut off management access to the switch.

Alternatively, the switch can be managed through the operational network, known as in-band management. Because in-band management traffic is mixed in with operational network traffic, it is subject to all of the filtering rules usually applied to a standard network ports such as ACLs and VLAN tagging. In-band network management can be accessed via a connection to any network port (1-52).

Setting an IP Address You must establish IP address information for the switch to obtain management access through the network. This can be done in either of the following ways:

- ◆ **Manual** — You have to input the information, including IP address and subnet mask. If your management station is not in the same IP subnet as the switch, you will also need to specify the default gateway router.
- ◆ **Dynamic** — The switch can send IPv4 configuration requests to BOOTP or DHCP address allocation servers on the network, or can automatically generate a unique IPv6 host address based on the local subnet address prefix received in router advertisement messages. An IPv6 link local address for use in a local network can also be dynamically generated as described in [“Obtaining an IPv6 Address” on page 64](#).

This switch is designed as a router, and therefore does not support DHCP for IPv6, so an IPv6 global unicast address for use in a network containing more than one subnet can only be manually configured as described in [“Assigning an IPv6 Address” on page 60](#).

Manual Configuration

You can manually assign an IP address to the switch. You may also need to specify a default gateway that resides between this device and management stations that exist on another network segment. Valid IPv4 addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the CLI program.



Note: The IPv4 address for the network interface on this switch is obtained via DHCP by default.

Assigning an IPv4 Address

Before you can assign an IP address to the switch, you must obtain the following information from your network administrator:

- ◆ IP address for the switch
- ◆ Network mask for this network
- ◆ Default gateway for the network

To assign an IPv4 address to the switch, complete the following steps

1. From the Global Configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.
2. Type “ip address *ip-address netmask*,” where “ip-address” is the switch IP address and “netmask” is the network mask for the network. Press <Enter>.
3. Type “exit” to return to the global configuration mode prompt. Press <Enter>.
4. To set the IP address of the default gateway for the network to which the switch belongs, type “ip default-gateway *gateway*,” where “gateway” is the IP address of the default gateway. Press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 192.168.1.254
```

Assigning an IPv6 Address

This section describes how to configure a “link local” address for connectivity within the local subnet only, and also how to configure a “global unicast” address, including a network prefix for use on a multi-segment network and the host portion of the address.

An IPv6 prefix or address must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used to indicate the appropriate number of zeros required to fill the undefined fields. For detailed information on the other ways to assign IPv6 addresses, see [“IPv6 Interface” on page 764](#).

Link Local Address — All link-local addresses must be configured with a prefix in the range of FE80~FEBF. Remember that this address type makes the switch accessible over IPv6 for all devices attached to the same local subnet only. Also, if the switch detects that the address you configured conflicts with that in use by another device on the subnet, it will stop using the address in question, and automatically generate a link local address that does not conflict with any other devices on the local subnet.

To configure an IPv6 link local address for the switch, complete the following steps:

1. From the Global Configuration mode prompt, type "interface vlan 1" to access the interface-configuration mode. Press <Enter>.
2. Type "ipv6 address" followed by up to 8 colon-separated 16-bit hexadecimal values for the *ipv6-address* similar to that shown in the example, followed by the "link-local" command parameter. Then press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address FE80::260:3EFF:FE11:6700 link-local
Console(config-if)#ipv6 enable
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
    fe80::260:3eff:fe11:6700%1/64
Global unicast address(es):
(None)
Joined group address(es):
ff02::2
ff02::1:ff00:0
ff02::1:ff11:6700
ff02::1:2
ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 1.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds

Console#
```

Address for Multi-segment Network — Before you can assign an IPv6 address to the switch that will be used to connect to a multi-segment network, you must obtain the following information from your network administrator:

- ◆ Prefix for this network
- ◆ IP address for the switch
- ◆ Default gateway for the network

For networks that encompass several different subnets, you must define the full address, including a network prefix and the host address for the switch. You can specify either the full IPv6 address, or the IPv6 address and prefix length. The prefix length for an IPv6 network is the number of bits (from the left) of the prefix that form the network address, and is expressed as a decimal number. For example, all IPv6 addresses that start with the first byte of 73 (hexadecimal) could be expressed as 73:0:0:0:0:0:0:0/8 or 73::/8.

To generate an IPv6 global unicast address for the switch, complete the following steps:

1. From the global configuration mode prompt, type "interface vlan 1" to access the interface-configuration mode. Press <Enter>.
2. From the interface prompt, type "ipv6 address *ipv6-address*" or "ipv6 address *ipv6-address/prefix-length*," where "prefix-length" indicates the address bits used to form the network portion of the address. (The network address starts from the left of the prefix and should encompass some of the ipv6-address bits.) The remaining bits are assigned to the host interface. Press <Enter>.
3. Type "exit" to return to the global configuration mode prompt. Press <Enter>.
4. To set the IP address of the IPv6 default gateway for the network to which the switch belongs, type "ipv6 default-gateway *gateway*," where "gateway" is the IPv6 address of the default gateway. Press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address 2001:DB8:2222:7272::/64
Console(config-if)#exit
Console(config)#ipv6 default-gateway 2001:DB8:2222:7272::254
Console(config)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
    fe80::260:3eff:fe11:6700%1/64
Global unicast address(es):
    2001:db8:2222:7272::/64, subnet is 2001:db8:2222:7272::/64
Joined group address(es):
    ff02::2
    ff02::1:ff00:0
    ff02::1:ff11:6700
    ff02::1:2
    ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 1.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds

Console#show ipv6 default-gateway
ipv6 default gateway: 2001:DB8:2222:7272::254
Console#
```

Dynamic Configuration

Obtaining an IPv4 Address

If you select the “bootp” or “dhcp” option, the system will immediately start broadcasting service requests. IP will be enabled but will not function until a BOOTP or DHCP reply has been received. Requests are broadcast every few minutes using exponential backoff until IP configuration information is obtained from a BOOTP or DHCP server. BOOTP and DHCP values can include the IP address, subnet mask, and default gateway. If the DHCP/BOOTP server is slow to respond, you may need to use the “ip dhcp restart client” command to re-start broadcasting service requests.

Note that the “ip dhcp restart client” command can also be used to start broadcasting service requests for all VLANs configured to obtain address assignments through BOOTP or DHCP. It may be necessary to use this command when DHCP is configured on a VLAN, and the member ports which were previously shut down are now enabled.

If the “bootp” or “dhcp” option is saved to the startup-config file (step 6), then the switch will start broadcasting service requests as soon as it is powered on.

To automatically configure the switch by communicating with BOOTP or DHCP address allocation servers on the network, complete the following steps:

- 1.** From the Global Configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.
- 2.** At the interface-configuration mode prompt, use one of the following commands:
 - To obtain IP settings via DHCP, type “ip address dhcp” and press <Enter>.
 - To obtain IP settings via BOOTP, type “ip address bootp” and press <Enter>.
- 3.** Type “end” to return to the Privileged Exec mode. Press <Enter>.
- 4.** Wait a few minutes, and then check the IP configuration settings by typing the “show ip interface” command. Press <Enter>.

5. Then save your configuration changes by typing “copy running-config startup-config.” Enter the startup file name and press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#end
Console#show ip interface
VLAN 1 is Administrative Up - Link Up
  Address is 00-E0-0C-00-00-FB
  Index: 1001, MTU: 1500
  Address Mode is DHCP
  IP Address: 192.168.0.2 Mask: 255.255.255.0
  Proxy ARP is disabled
Console#copy running-config startup-config
Startup configuration file name []: startup
\Write to FLASH Programming.

\Write to FLASH finish.
Success.
```

Obtaining an IPv6 Address

Link Local Address — There are several ways to configure IPv6 addresses. The simplest method is to automatically generate a “link local” address (identified by an address prefix in the range of FE80~FEBF). This address type makes the switch accessible over IPv6 for all devices attached to the same local subnet.

To generate an IPv6 link local address for the switch, complete the following steps:

1. From the Global Configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.
2. Type “ipv6 enable” and press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 enable
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled
Link-local address:
  FE80::260:3EFF:FE11:6700/64
Global unicast address(es):
  2001:DB8:2222:7272::/64, subnet is 2001:DB8:2222:7272::/64
Joined group address(es):
  FF02::1:FF00:0
  FF02::1:FF11:6700
  FF02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 1.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds

Console#
```

Enabling SNMP Management Access

The switch can be configured to accept management commands from Simple Network Management Protocol (SNMP) applications such as Edge-Core ECView Pro. You can configure the switch to respond to SNMP requests or generate SNMP traps.

When SNMP management stations send requests to the switch (either to return information or to set a parameter), the switch provides the requested data or sets the specified parameter. The switch can also be configured to send information to SNMP managers (without being requested by the managers) through trap messages, which inform the manager that certain events have occurred.

The switch includes an SNMP agent that supports SNMP version 1, 2c, and 3 clients. To provide management access for version 1 or 2c clients, you must specify a community string. The switch provides a default MIB View (i.e., an SNMPv3 construct) for the default “public” community string that provides read access to the entire MIB tree, and a default view for the “private” community string that provides read/write access to the entire MIB tree. However, you may assign new views to version 1 or 2c community strings that suit your specific security requirements (see [snmp-server view](#) command).

Community Strings (for SNMP version 1 and 2c clients)

Community strings are used to control management access to SNMP version 1 and 2c stations, as well as to authorize SNMP stations to receive trap messages from the switch. You therefore need to assign community strings to specified users, and set the access level.

The default strings are:

- ◆ **public** - with read-only access. Authorized management stations are only able to retrieve MIB objects.
- ◆ **private** - with read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

To prevent unauthorized access to the switch from SNMP version 1 or 2c clients, it is recommended that you change the default community strings.

To configure a community string, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type “snmp-server community *string mode*,” where “string” is the community access string and “mode” is **rw** (read/write) or **ro** (read only). Press <Enter>. (Note that the default mode is read only.)
2. To remove an existing string, simply type “no snmp-server community *string*,” where “string” is the community access string to remove. Press <Enter>.

```
Console(config)#snmp-server community admin rw
Console(config)#snmp-server community private
Console(config)#
```



Note: If you do not intend to support access to SNMP version 1 and 2c clients, we recommend that you delete both of the default community strings. If there are no community strings, then SNMP management access from SNMP v1 and v2c clients is disabled.

Trap Receivers

You can also specify SNMP stations that are to receive traps from the switch. To configure a trap receiver, use the “snmp-server host” command. From the Privileged Exec level global configuration mode prompt, type:

```
“snmp-server host host-address community-string [version {1 | 2c | 3 {auth |
noauth | priv}}]”
```

where “host-address” is the IP address for the trap receiver, “community-string” specifies access rights for a version 1/2c host, or is the user name of a version 3 host, “version” indicates the SNMP client version, and “auth | noauth | priv” means that authentication, no authentication, or authentication and privacy is used for v3 clients. Then press <Enter>. For a more detailed description of these parameters, see the [snmp-server host](#) command. The following example creates a trap host for each type of SNMP client.

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#snmp-server host 10.1.19.98 robin version 2c
Console(config)#snmp-server host 10.1.19.34 barbie version 3 auth
Console(config)#
```

Configuring Access for SNMP Version 3 Clients

To configure management access for SNMPv3 clients, you need to first create a view that defines the portions of MIB that the client can read or write, assign the view to a group, and then assign the user to a group. The following example creates one view called “mib-2” that includes the entire MIB-2 tree branch, and then another view that includes the IEEE 802.1d bridge MIB. It assigns these respective read and read/write views to a group call “r&d” and specifies group authentication via MD5 or SHA. In the last step, it assigns a v3 user to this group, indicating that MD5 will be used for authentication, provides the password “greenpeace” for authentication, and the password “einstien” for encryption.

```
Console(config)#snmp-server view mib-2 1.3.6.1.2.1 included
Console(config)#snmp-server view 802.1d 1.3.6.1.2.1.17 included
Console(config)#snmp-server group r&d v3 auth mib-2 802.1d
```

```
Console(config)#snmp-server user steve group r&d v3 auth md5 greenpeace priv  
des56 einstien  
Console(config)#
```

For a more detailed explanation on how to configure the switch for access from SNMP v3 clients, refer to the *CLI Reference Guide* or *Web Management Guide*.

Managing System Files

The switch's flash memory supports three types of system files that can be managed by the CLI program, the web interface, or SNMP. The switch's file system allows files to be uploaded and downloaded, copied, deleted, and set as a start-up file.

The types of files are:

- ◆ **Configuration** — This file type stores system configuration information and is created when configuration settings are saved. Saved configuration files can be selected as a system start-up file or can be uploaded via FTP/TFTP to a server for backup. The file named "Factory_Default_Config.cfg" contains all the system default settings and cannot be deleted from the system. If the system is booted with the factory default settings, the switch will also create a file named "startup1.cfg" that contains system settings for switch initialization, including information about the unit identifier, and MAC address for the switch. The configuration settings from the factory defaults configuration file are copied to this file, which is then used to boot the switch. See ["Saving or Restoring Configuration Settings" on page 68](#) for more information.
- ◆ **Operation Code** — System software that is executed after boot-up, also known as run-time code. This code runs the switch operations and provides the CLI and web management interfaces.
- ◆ **Diagnostic Code** — Software that is run during system boot-up, also known as POST (Power On Self-Test).



Note: The Boot ROM and Loader cannot be uploaded or downloaded from the FTP/TFTP server. You must follow the instructions in the release notes for new firmware, or contact your distributor for help.

Due to the size limit of the flash memory, the switch supports only two operation code files. However, you can have as many diagnostic code files and configuration files as available flash memory space allows. The switch has a total of 2 GB of flash memory for system files.

In the system flash memory, one file of each type must be set as the start-up file. During a system boot, the diagnostic and operation code files set as the start-up file are run, and then the start-up configuration file is loaded.

Note that configuration files should be downloaded using a file name that reflects the contents or usage of the file settings. If you download directly to the running-config, the system will reboot, and the settings will have to be copied from the running-config to a permanent file.

Upgrading the Operation Code

The following example shows how to download new firmware to the switch and activate it. The TFTP server could be any standards-compliant server running on Windows or Linux. When downloading from an FTP server, the logon interface will prompt for a user name and password configured on the remote server. Note that “anonymous” is set as the default user name.

File names on the switch are case-sensitive. The destination file name should not contain slashes (\ or /), and the maximum length for file names is 32 characters for files on the switch or 128 characters for files on the server. (Valid characters: A-Z, a-z, 0-9, “,” “-”)

```
Console#copy tftp file
TFTP server ip address: 10.1.0.19
Choose file type:
1. config: 2. opcode: 2
Source file name: m360.bix
Destination file name: m360.bix
\Write to FLASH Programming.
-Write to FLASH finish.
Success.
Console#config
Console(config)#boot system opcode: m360.bix
Console(config)#exit
Console#dir
```

File Name	Type	Startup	Modify Time	Size(bytes)
Unit 1:				
m360.bix	OpCode	Y	2013-02-25 15:41:04	25812529
m355.bix	OpCode	N	2012-12-04 13:23:59	25783857
Factory_Default_Config.cfg	Config	N	2012-12-04 13:18:37	455
startup1.cfg	Config	Y	2013-03-21 05:39:15	3463

```
-----
Free space for compressed user config files:1593241600
Console#
```

Saving or Restoring Configuration Settings

Configuration commands only modify the running configuration file and are not saved when the switch is rebooted. To save all your configuration changes in nonvolatile storage, you must copy the running configuration file to the start-up configuration file using the “copy” command.

New startup configuration files must have a name specified. File names on the switch are case-sensitive, can be from 1 to 31 characters, must not contain slashes

(\ or /), and the leading letter of the file name must not be a period (.). (Valid characters: A-Z, a-z, 0-9, ",", "-", "_")

There can be more than one user-defined configuration file saved in the switch's flash memory, but only one is designated as the "startup" file that is loaded when the switch boots. The **copy running-config startup-config** command always sets the new file as the startup file. To select a previously saved configuration file, use the **boot system config:<filename>** command.

The maximum number of saved configuration files depends on available flash memory. The amount of available flash memory can be checked by using the **dir** command.

To save the current configuration settings, enter the following command:

1. From the Privileged Exec mode prompt, type "copy running-config startup-config" and press <Enter>.
2. Enter the name of the start-up file. Press <Enter>.

```
Console#copy running-config startup-config
Startup configuration file name []: startup
\Write to FLASH Programming.

\Write to FLASH finish.
Success.

Console#
```

To restore configuration settings from a backup server, enter the following command:

1. From the Privileged Exec mode prompt, type "copy tftp startup-config" and press <Enter>.
2. Enter the address of the TFTP server. Press <Enter>.
3. Enter the name of the startup file stored on the server. Press <Enter>.
4. Enter the name for the startup file on the switch. Press <Enter>.

```
Console#copy tftp startup-config
TFTP server IP address: 192.168.0.4
Source configuration file name: startup-rd.cfg
Startup configuration file name [startup1.cfg]:

Success.
Console#
```

Configuring Automatic Installation of Operation Code and Configuration Settings

Downloading Operation Code from a File Server

Automatic Operation Code Upgrade can automatically download an operation code file when a file newer than the currently installed one is discovered on the file server. After the file is transferred from the server and successfully written to the file system, it is automatically set as the startup file, and the switch is rebooted.

Usage Guidelines

- ◆ If this feature is enabled, the switch searches the defined URL once during the bootup sequence.
- ◆ FTP (port 21) and TFTP (port 69) are both supported. Note that the TCP/UDP port bindings cannot be modified to support servers listening on non-standard ports.
- ◆ The host portion of the upgrade file location URL must be a valid IPv4 IP address. DNS host names are not recognized. Valid IP addresses consist of four numbers, 0 to 255, separated by periods.
- ◆ The path to the directory must also be defined. If the file is stored in the root directory for the FTP/TFTP service, then use the "/" to indicate this (e.g., ftp://192.168.0.1/).
- ◆ The file name must not be included in the upgrade file location URL. The file name of the code stored on the remote server must be `ecs5610-52s.bix` (using lower case letters as indicated).
- ◆ The FTP connection is made with PASV mode enabled. PASV mode is needed to traverse some fire walls, even if FTP traffic is not blocked. PASV mode cannot be disabled.
- ◆ The switch-based search function is case-insensitive in that it will accept a file name in upper or lower case (i.e., the switch will accept `ECS5610-52S.BIX` from the server even though `ECS5610-52S.bix` was requested). However, keep in mind that the file systems of many operating systems such as Unix and most Unix-like systems (FreeBSD, NetBSD, OpenBSD, and most Linux distributions, etc.) are case-sensitive, meaning that two files in the same directory, `ecs5610-52s.bix` and `ECS5610-52S.BIX` are considered to be unique files. Thus, if the upgrade file is stored as `ECS5610-52S.BIX` (or even `Ecs5610-52s.bix`) on a case-sensitive server, then the switch (requesting `ECS5610-52S.bix`) will not be upgraded because the server does not recognize the requested file name and the stored file name as being equal. A notable exception in the list of case-sensitive Unix-like operating systems is Mac OS X, which by default is case-insensitive. Please check the documentation for your server's operating system if you are unsure of its file system's behavior.

- ◆ Note that the switch itself does not distinguish between upper and lower-case file names, and only checks to see if the file stored on the server is more recent than the current runtime image.
- ◆ If two operation code image files are already stored on the switch's file system, then the non-startup image is deleted before the upgrade image is transferred.
- ◆ The automatic upgrade process will take place in the background without impeding normal operations (data switching, etc.) of the switch.
- ◆ During the automatic search and transfer process, the administrator cannot transfer or update another operation code image, configuration file, public key, or HTTPS certificate (i.e., no other concurrent file management operations are possible).
- ◆ The upgrade operation code image is set as the startup image after it has been successfully written to the file system.
- ◆ The switch will send an SNMP trap and make a log entry upon all upgrade successes and failures.
- ◆ The switch will immediately restart after the upgrade file is successfully written to the file system and set as the startup image.

To enable automatic upgrade, enter the following commands:

1. Specify the TFTP or FTP server to check for new operation code.

- When specifying a TFTP server, the following syntax must be used, where *filedir* indicates the path to the directory containing the new image:

```
tftp://192.168.0.1[/filedir]/
```

- When specifying an FTP server, the following syntax must be used, where *filedir* indicates the path to the directory containing the new image:

```
ftp://[username[:password@]]192.168.0.1[/filedir]/
```

If the user name is omitted, "anonymous" will be used for the connection. If the password is omitted a null string ("") will be used for the connection.

This shows how to specify a TFTP server where new code is stored.

```
Console(config)#upgrade opcode path tftp://192.168.0.1/sm24/
Console(config)#
```

This shows how to specify an FTP server where new code is stored.

```
Console(config)#upgrade opcode path ftp://admin:billy@192.168.0.1/sm24/
Console(config)#
```

2. Set the switch to automatically reboot and load the new code after the opcode upgrade is completed.

```
Console(config)#upgrade opcode reload
Console(config)#
```

3. Set the switch to automatically upgrade the current operational code when a new version is detected on the server. When the switch starts up and automatic image upgrade is enabled by this command, the switch will follow these steps when it boots up:
 - a. It will search for a new version of the image at the location specified by **upgrade opcode path** command. The name for the new image stored on the TFTP server must be ecs5610_52s.bix. If the switch detects a code version newer than the one currently in use, it will download the new image. If two code images are already stored in the switch, the image not set to start up the system will be overwritten by the new version.
 - b. After the image has been downloaded, the switch will send a trap message to log whether or not the upgrade operation was successful.
 - c. It sets the new version as the startup image.
 - d. It then restarts the system to start using the new image.

```
Console(config)#upgrade opcode auto
Console(config)#
```

4. Display the automatic upgrade settings.

```
Console#show upgrade
Auto Image Upgrade Global Settings:
  Status      : Enabled
  Reload Status : Enabled
  Path        :
  File Name   : ecs5610-52s.bix
Console#
```

Specifying a DHCP Client Identifier

DHCP servers index their database of address bindings using the client's Media Access Control (MAC) Address or a unique client identifier. The client identifier is used to identify the vendor class and configuration of the switch to the DHCP server, which then uses this information to decide on how to service the client or the type of information to return.

DHCP client Identifier (Option 60) is used by DHCP clients to specify their unique identifier. The client identifier is optional and can be specified while configuring DHCP on the primary network interface. DHCP Option 60 is disabled by default.

The general framework for this DHCP option is set out in RFC 2132 (Option 60). This information is used to convey configuration settings or other identification information about a client, but the specific string to use should be supplied by your service provider or network administrator. Options 60 (vendor-class-identifier), 66 (tftp-server-name) and 67 (bootfile-name) statements can be added to the server daemon's configuration file as described in the following section.

If the DHCP server has an index entry for a switch requesting service, it should reply with the TFTP server name and boot file name. Note that the vendor class identifier can be formatted in either text or hexadecimal, but the format used by both the client and server must be the same.

```
Console(config)#interface vlan 2
Console(config-if)#ip dhcp client class-id hex 0000e8666572
Console(config-if)#
```

Downloading a Configuration File Referenced by a DHCP Server

Information passed on to the switch from a DHCP server may also include a configuration file to be downloaded and the TFTP servers where that file can be accessed. If the Factory Default Configuration file is used to provision the switch at startup, in addition to requesting IP configuration settings from the DHCP server, it will also ask for the name of a bootup configuration file and TFTP servers where that file is stored.

If the switch receives information that allows it to download the remote bootup file, it will save this file to a local buffer, and then restart the provision process.

Note the following DHCP client behavior:

- ◆ The bootup configuration file received from a TFTP server is stored on the switch with the original file name. If this file name already exists in the switch, the file is overwritten.
- ◆ If the name of the bootup configuration file is the same as the Factory Default Configuration file, the download procedure will be terminated, and the switch will not send any further DHCP client requests.
- ◆ If the switch fails to download the bootup configuration file based on information passed by the DHCP server, it will not send any further DHCP client requests.
- ◆ If the switch does not receive a DHCP response prior to completing the bootup process, it will continue to send a DHCP client request once a minute. These requests will only be terminated if the switch's address is manually configured, but will resume if the address mode is set back to DHCP.

To successfully transmit a bootup configuration file to the switch, the DHCP daemon (using a Linux based system for this example) must be configured with the following information:

- ◆ Options 60, 66 and 67 statements can be added to the daemon's configuration file.

Table 1: Options 60, 66 and 67 Statements

Option	Statement	
	Keyword	Parameter
60	vendor-class-identifier	a string indicating the vendor class identifier
66	tftp-server-name	a string indicating the tftp server name
67	bootfile-name	a string indicating the bootfile name

- ◆ By default, DHCP option 66/67 parameters are not carried in a DHCP server reply. To ask for a DHCP reply with option 66/67 information, the DHCP client request sent by this switch includes a "parameter request list" asking for this information. Besides these items, the client request also includes a "vendor class identifier" that allows the DHCP server to identify the device, and select the appropriate configuration file for download. This information is included in Option 55 and 124.

Table 2: Options 55 and 124 Statements

Option	Statement	
	Keyword	Parameter
55	dhcp-parameter-request-list	a list of parameters, separated by a comma ','
124	vendor-class-identifier	a string indicating the vendor class identifier

The following configuration example is provided for a Linux-based DHCP daemon (dhcpd.conf file). In the "Vendor class" section, the server will always send Option 66 and 67 to tell the switch to download the "test" configuration file from server 192.168.255.101.

```
ddns-update-style ad-hoc;

default-lease-time 600;
max-lease-time 7200;

log-facility local7;

server-name "Server1";
Server-identifier 192.168.255.250;
#option 66, 67
option space dynamicProvision code width 1 length 1 hash size 2;
option dynamicProvision.tftp-server-name code 66 = text;
option dynamicProvision.bootfile-name code 67 = text;

subnet 192.168.255.0 netmask 255.255.255.0 {
```

```
range 192.168.255.160 192.168.255.200;
option routers 192.168.255.101;
option tftp-server-name "192.168.255.100"; #Default Option 66
option bootfile-name "bootfile";          #Default Option 67
}

class "Option66,67_1" {                    #DHCP Option 60 Vendor class
two
match if option vendor-class-identifier = "ecs5610-52s.cfg";
option tftp-server-name "192.168.255.101";
option bootfile-name "test";
}
```



Note: Use "ecs5610-52s.cfg" for the vendor-class-identifier in the dhcpd.conf file.

Setting the System Clock

Simple Network Time Protocol (SNTP) or Network Time Protocol (NTP) can be used to set the switch's internal clock based on periodic updates from a time server. Maintaining an accurate time on the switch enables the system log to record meaningful dates and times for event entries. You can also manually set the clock. If the clock is not set manually or via SNTP or NTP, the switch will only record the time from the factory default set at the last bootup.

When the SNTP client is enabled, the switch periodically sends a request for a time update to a configured time server. You can configure up to three time server IP addresses. The switch will attempt to poll each server in the configured sequence.

The switch also supports the following time settings:

- ◆ Time Zone – You can specify the offset from Coordinated Universal Time (UTC), also known as Greenwich Mean Time (GMT).
- ◆ Summer Time/Daylight Saving Time (DST) – In some regions, the time shifts by one hour in the fall and spring. The switch supports manual entry for one-time or recurring clock shifts.

Setting the Time Manually

To manually set the clock to 14:11:36, April 1st, 2013, enter this command.

```
Console#calendar set 14 11 36 1 April 2013
Console#
```

To set the time zone, enter a command similar to the following.

```
Console(config)#clock timezone Japan hours 8 after-UTC
Console(config)#
```

To set the time shift for summer time, enter a command similar to the following.

```
Console(config)#clock summer-time SUMMER date 2 april 2013 0 0 30 june 2013 0
0
Console(config)#
```

To display the clock configuration settings, enter the following command.

```
Console#show calendar
Current Time       : Apr  2 15:56:12 2013
Time Zone          : UTC, 08:00
Summer Time        : SUMMER, offset 60 minutes
                   Apr 2 2013 00:00 to Jun 30 2013 00:00
Summer Time in Effect : Yes
Console#
```

Configuring SNTP Setting the clock based on an SNTP server can provide more accurate clock synchronization across network switches than manually-configured time. To configure SNTP, set the switch as an SNTP client, and then set the polling interval, and specify a time server as shown in the following example.

```
Console(config)#sntp client
Console(config)#sntp poll 60
Console(config)#sntp server 10.1.0.19
Console(config)#exit
Console#show sntp
Current Time       : Apr  2 16:06:07 2013
Poll Interval      : 60 seconds
Current Mode       : Unicast
SNTP Status        : Enabled
SNTP Server        : 10.1.0.19
Current Server     : 10.1.0.19
Console#
```

Configuring NTP Requesting the time from an NTP server is the most secure method. You can enable NTP authentication to ensure that reliable updates are received from only authorized NTP servers. The authentication keys and their associated key number must be centrally managed and manually distributed to NTP servers and clients. The key numbers and key values must match on both the server and client.

When more than one time server is configured, the client will poll all of the time servers, and compare the responses to determine the most reliable and accurate time update for the switch.

To configure NTP time synchronization, enter commands similar to the following.

```
Console(config)#ntp client
Console(config)#ntp authentication-key 45 md5 thisiskey45
Console(config)#ntp authenticate
Console(config)#ntp server 192.168.3.20
```

```
Console(config)#ntp server 192.168.3.21
Console(config)#ntp server 192.168.5.23 key 19
Console(config)#exit
Console#show ntp
Current Time           : Apr 29 13:57:32 2011
Polling                : 1024 seconds
Current Mode           : unicast
NTP Status              : Enabled
NTP Authenticate Status : Enabled
Last Update NTP Server  : 192.168.0.88      Port: 123
Last Update Time        : Mar 12 02:41:01 2013 UTC
NTP Server 192.168.0.88 version 3
NTP Server 192.168.3.21 version 3
NTP Server 192.168.4.22 version 3 key 19
NTP Authentication Key 19 md5 42V68751663T6K11P2J307210R885

Current Time           : Apr  2 16:28:34 2013
Polling                : 1024 seconds
Current Mode           : unicast
NTP Status              : Enabled
NTP Authenticate Status : Enabled
Last Update NTP Server  : 192.168.5.23      Port: 0
Last Update Time        : Apr  2 16:00:00 2013 UTC
NTP Server 192.168.3.20 version 3
NTP Server 192.168.3.21 version 3
NTP Server 192.168.5.23 version 3 key 19
NTP Authentication Key 45 md5 2662T75S5658RU5424180034777
Console#
```

Section II

Command Line Interface

This section provides a detailed description of the Command Line Interface, along with examples for all of the commands.

This section includes these chapters:

- ◆ ["Using the Command Line Interface" on page 81](#)
- ◆ ["General Commands" on page 93](#)
- ◆ ["System Management Commands" on page 101](#)
- ◆ ["SNMP Commands" on page 179](#)
- ◆ ["Remote Monitoring Commands" on page 201](#)
- ◆ ["Flow Sampling Commands" on page 209](#)
- ◆ ["Authentication Commands" on page 217](#)
- ◆ ["General Security Measures" on page 275](#)
- ◆ ["Access Control Lists" on page 347](#)
- ◆ ["Interface Commands" on page 369](#)
- ◆ ["Link Aggregation Commands" on page 401](#)
- ◆ ["Port Mirroring Commands" on page 415](#)
- ◆ ["Congestion Control Commands" on page 425](#)
- ◆ ["Address Table Commands" on page 443](#)
- ◆ ["Spanning Tree Commands" on page 449](#)
- ◆ ["VLAN Commands" on page 477](#)
- ◆ ["Class of Service Commands" on page 527](#)

- ◆ [“Quality of Service Commands” on page 547](#)
- ◆ [“Multicast Filtering Commands” on page 591](#)
- ◆ [“LLDP Commands” on page 695](#)
- ◆ [“Domain Name Service Commands” on page 721](#)
- ◆ [“DHCP Commands” on page 729](#)
- ◆ [“IP Interface Commands” on page 749](#)
- ◆ [“VRRP Commands” on page 801](#)
- ◆ [“IP Routing Commands” on page 811](#)
- ◆ [“Multicast Routing Commands” on page 1011](#)

2

Using the Command Line Interface

This chapter describes how to use the Command Line Interface (CLI).

Accessing the CLI

When accessing the management interface for the switch over a direct connection to the server's console port, or via a Telnet or Secure Shell connection (SSH), the switch can be managed by entering command keywords and parameters at the prompt. Using the switch's command-line interface (CLI) is very similar to entering commands on a UNIX system.

Console Connection To access the switch through the console port, perform these steps:

1. At the console prompt, enter the user name and password. (The default user names are "admin" and "guest" with corresponding passwords of "admin" and "guest.") When the administrator user name and password is entered, the CLI displays the "Console#" prompt and enters privileged access mode (i.e., Privileged Exec). But when the guest user name and password is entered, the CLI displays the "Console>" prompt and enters normal access mode (i.e., Normal Exec).
2. Enter the necessary commands to complete your desired tasks.
3. When finished, exit the session with the "quit" or "exit" command.

After connecting to the system through the console port, the login screen displays:

```
User Access Verification
Username: admin
Password:
  CLI session with the ECS5610-52S is opened.
  To end the CLI session, enter [Exit].
Console#
```

Telnet Connection Telnet operates over the IP transport protocol. In this environment, your management station and any network device you want to manage over the network must have a valid IP address. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Each address consists of a network portion and host

portion. For example, the IP address assigned to this switch, 10.1.0.1, consists of a network portion (10.1.0) and a host portion (1).



Note: The IP address for this switch is obtained via DHCP by default.

To access the switch through a Telnet session, you must first set the IP address for the Master unit, and set the default gateway if you are managing the switch from a different IP subnet. For example,

```
Console(config)#interface vlan 1
Console(config-if)#ip address 10.1.0.254 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254
Console(config)#
```

If your corporate network is connected to another network outside your office or to the Internet, you need to apply for a registered IP address. However, if you are attached to an isolated network, then you can use any IP address that matches the network segment to which you are attached.

After you configure the switch with an IP address, you can open a Telnet session by performing these steps:

1. From the remote host, enter the Telnet command and the IP address of the device you want to access.
2. At the prompt, enter the user name and system password. The CLI will display the "Vty-*n*#" prompt for the administrator to show that you are using privileged access mode (i.e., Privileged Exec), or "Vty-*n*>" for the guest to show that you are using normal access mode (i.e., Normal Exec), where *n* indicates the number of the current Telnet session.
3. Enter the necessary commands to complete your desired tasks.
4. When finished, exit the session with the "quit" or "exit" command.

After entering the Telnet command, the login screen displays:

```
Username: admin
Password:

CLI session with the ECS5610-52S is opened.
To end the CLI session, enter [Exit].

Vty-0#
```



Note: You can open up to eight sessions to the device via Telnet or SSH.

Entering Commands

This section describes how to enter CLI commands.

Keywords and Arguments A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command “show interfaces status ethernet 1/5,” **show interfaces** and **status** are keywords, **ethernet** is an argument that specifies the interface type, and **1/5** specifies the unit/port.

You can enter commands as follows:

- ◆ To enter a simple command, enter the command keyword.
- ◆ To enter multiple commands, enter each command in the required order. For example, to enable Privileged Exec command mode, and display the startup configuration, enter:

```
Console>enable  
Console#show startup-config
```

- ◆ To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:

```
Console(config)#username admin password 0 smith
```

Minimum Abbreviation The CLI will accept a minimum number of characters that uniquely identify a command. For example, the command “configure” can be entered as **con**. If an entry is ambiguous, the system will prompt for further input.

Command Completion If you terminate input with a Tab key, the CLI will print the remaining characters of a partial keyword up to the point of ambiguity. In the “logging history” example, typing **log** followed by a tab will result in printing the command up to “**logging**.”

Getting Help on Commands You can display a brief description of the help system by entering the **help** command. You can also display command syntax by using the "?" character to list keywords or parameters.

Showing Commands

If you enter a "?" at the command prompt, the system will display the first level of keywords or command groups. You can also display a list of valid keywords for a specific command. For example, the command "**show ?**" displays a list of possible show commands:

```
Console#show ?
  access-group      Access groups
  access-list       Access lists
  accounting        Uses an accounting list with this name
  arp              Information of ARP cache
  authorization     Enables EXEC accounting
  auto-traffic-control Auto traffic control information
  banner            Banner info
  bridge-ext        Bridge extension information
  calendar          Date and time information
  class-map         Displays class maps
  cluster           Display cluster
  cn                Displays congestion notification information
  dcbx              DCBX
  debug            State of each debugging option
  dns              DNS information
  dos-protection    Shows the system dos-protection summary information
  dot1q-tunnel      dot1q-tunnel
  dot1x            802.1X content
  ets              802.1Qaz configuration
  garp             GARP properties
  gvrp             GVRP interface information
  history           Shows history information
  hosts            Host information
  interfaces        Shows interface information
  ip               IP information
  ipv6             IPv6 information
  l2protocol-tunnel Layer 2 protocol tunneling configuration
  lacp             LACP statistics
  line             TTY line information
  lldp             LLDP
  location-led      Location LED operation
  log              Log records
  logging          Logging setting
  loop             Shows the information of loopback
  mac              MAC access list
  mac-address-table Configuration of the address table
  mac-vlan         MAC-based VLAN information
  management       Shows management information
  memory           Memory utilization
  mvr             Multicast vlan registration
  mvr6            IPv6 Multicast VLAN registration
  network-access   Shows the entries of the secure port.
  nlm             Show notification log
  ntp             Network Time Protocol configuration
  pfc             Displays Priority-based Flow Control Information
  policy-map       Displays policy maps
  port            Port characteristics
  port-channel     Port channel information
  pppoe           Displays PPPoE configuration
```

```
process                Device process
protocol-vlan          Protocol-VLAN information
public-key             Public key information
qos                   Quality of Service
queue                 Priority queue information
radius-server          RADIUS server information
reload                Shows the reload settings
rmon                  Remote Monitoring Protocol
route-map              Shows route-map
rspan                 Display status of the current RSPAN configuration
running-config         Information on the running configuration
sflow                 Shows the sflow information
snmp                  Simple Network Management Protocol configuration and
                      statistics
sntp                  Simple Network Time Protocol configuration
spanning-tree          Spanning-tree configuration
ssh                   Secure shell server connections
startup-config         Startup system configuration
subnet-vlan            IP subnet-based VLAN information
synce                  Shows synchronous ethernet status
system                System information
tacacs-server          TACACS server information
tech-support           Technical information
time-range             Time range
traffic-segmentation   Traffic segmentation information
upgrade               Shows upgrade information
users                 Information about users logged in
version               System hardware and software versions
vlan                  Shows virtual LAN settings
vlan-translation       VLAN translation information
voice                  Shows the voice VLAN information
vrrp                  Shows VRRP
watchdog               Displays watchdog status
web-auth               Shows web authentication configuration
Console#show
```

The command “**show interfaces ?**” will display the following information:

```
Console#show interfaces ?
brief                Brief interface description
counters             Interface counters information
history              Historical sample of interface counters information
protocol-vlan        Protocol-VLAN information
status               Shows interface status
switchport           Shows interface switchport information
transceiver          Interface of transceiver information
transceiver-threshold Interface of transceiver-threshold information
Console#
```

Show commands which display more than one page of information (e.g., **show running-config**) pause and require you to press the [Space] bar to continue displaying one more page, the [Enter] key to display one more line, or the [a] key to display the rest of the information without stopping. You can press any other key to terminate the display.

Partial Keyword Lookup If you terminate a partial keyword with a question mark, alternatives that match the initial letters are provided. (Remember not to leave a space between the command and question mark.) For example “**s?**” shows all the keywords starting with “s.”

```
Console#show s?  
sflow          snmp          snmp          spanning-tree  ssh  
startup-config subnet-vlan  system  
Console#show s
```

Negating the Effect of Commands For many configuration commands you can enter the prefix keyword “**no**” to cancel the effect of a command or reset the configuration to the default value. For example, the **logging** command will log system messages to a host server. To disable logging, specify the **no logging** command. This guide describes the negation effect for all applicable commands.

Using Command History The CLI maintains a history of commands that have been entered. You can scroll back through the history of commands by pressing the up arrow key. Any command displayed in the history list can be executed again, or first modified and then executed.

Using the **show history** command displays a longer list of recently executed commands.

Understanding Command Modes The command set is divided into Exec and Configuration classes. Exec commands generally display information on system status or clear statistical counters. Configuration commands, on the other hand, modify interface parameters or enable certain switching functions. These classes are further divided into different modes. Available commands depend on the selected mode. You can always enter a question mark “**?**” at the prompt to display a list of the commands available for the current mode. The command classes and associated modes are displayed in the following table:

Table 3: General Command Modes

Class	Mode
Exec	Normal Privileged
Configuration	Global* Access Control List Class Map DHCP IGMP Profile Interface Line Multiple Spanning Tree Policy Map Route Map Router Time Range VLAN Database

* You must be in Privileged Exec mode to access the Global configuration mode.
You must be in Global Configuration mode to access any of the other configuration modes.

Exec Commands When you open a new console session on the switch with the user name and password “guest,” the system enters the Normal Exec command mode (or guest mode), displaying the “Console>” command prompt. Only a limited number of the commands are available in this mode. You can access all commands only from the Privileged Exec command mode (or administrator mode). To access Privilege Exec mode, open a new console session with the user name and password “admin.” The system will now display the “Console#” command prompt. You can also enter Privileged Exec mode from within Normal Exec mode, by entering the [enable](#) command, followed by the privileged level password “super.”

To enter Privileged Exec mode, enter the following user names and passwords:

```
Username: admin
Password: [admin login password]

CLI session with the ECS5610-52S is opened.
To end the CLI session, enter [Exit].

Console#
```

```
Username: guest
Password: [guest login password]

CLI session with the ECS5610-52S is opened.
To end the CLI session, enter [Exit].

Console>enable
Password: [privileged level password]
Console#
```

Configuration Commands Configuration commands are privileged level commands used to modify switch settings. These commands modify the running configuration only and are not saved when the switch is rebooted. To store the running configuration in non-volatile storage, use the **copy running-config startup-config** command.

The configuration commands are organized into different modes:

- ◆ Global Configuration - These commands modify the system level configuration, and include commands such as **hostname** and **snmp-server community**.
- ◆ Access Control List Configuration - These commands are used for packet filtering.
- ◆ CFM Configuration - Configures connectivity monitoring using continuity check messages, fault verification through loopback messages, and fault isolation by examining end-to-end connections between Provider Edge devices or between Customer Edge devices.
- ◆ Class Map Configuration - Creates a DiffServ class map for a specified traffic type.
- ◆ DHCP Configuration - These commands are used to configure the DHCP server.
- ◆ IGMP Profile - Sets a profile group and enters IGMP filter profile configuration mode.
- ◆ Interface Configuration - These commands modify the port configuration such as **speed-duplex** and **negotiation**.
- ◆ Line Configuration - These commands modify the console port and Telnet configuration, and include command such as **parity** and **databits**.
- ◆ Multiple Spanning Tree Configuration - These commands configure settings for the selected multiple spanning tree instance.
- ◆ Policy Map Configuration - Creates a DiffServ policy map for multiple interfaces.
- ◆ Route Map Configuration - These commands specify the action (next hop or silently drop) to take when a match is found.
- ◆ Router Configuration - These commands configure global settings for unicast and multicast routing protocols.
- ◆ Time Range - Sets a time range for use by other functions, such as Access Control Lists.
- ◆ VLAN Configuration - Includes the command to create VLAN groups.

To enter the Global Configuration mode, enter the command **configure** in Privileged Exec mode. The system prompt will change to "Console(config)#" which gives you access privilege to all Global Configuration commands.

```
Console#configure
Console(config)#
```

To enter the other modes, at the configuration prompt type one of the following commands. Use the **exit** or **end** command to return to the Privileged Exec mode.

Table 4: Configuration Command Modes

Mode	Command	Prompt	Page
Access Control List	access-list arp	Console(config-arp-acl)	364
	access-list ip standard	Console(config-std-acl)	348
	access-list ip extended	Console(config-ext-acl)	348
	access-list ipv6 standard	Console(config-std-ipv6-acl)	354
	access-list ipv6 extended	Console(config-ext-ipv6-acl)	354
	access-list mac	Console(config-mac-acl)	359
Class Map	class-map	Console(config-cmap)	548
DHCP	ip dhcp pool	Console(config-dhcp)	738
Interface	interface {ethernet <i>port</i> port-channel <i>id</i> vlan <i>id</i> }	Console(config-if)	370
Line	line {console vty}	Console(config-line)	135
MSTP	spanning-tree mst-configuration	Console(config-mstp)	456
Policy Map	policy-map	Console(config-pmap)	551
Time Range	time-range	Console(config-time-range)	169
Route Map	route-map	Console(config-route-map)	990
Router	router {bgp ipv6 ospf ospf pim pim6 rip}	Console(config-router)	907
			882
			840
			1020
			1043
			822
Time Range	time-range	Console(config-time-range)	169
VLAN	vlan database	Console(config-vlan)	484

For example, you can use the following commands to enter interface configuration mode, and then return to Privileged Exec mode

```
Console(config)#interface ethernet 1/5
.
.
Console(config-if)#exit
Console(config)#
```

Command Line Processing

Commands are not case sensitive. You can abbreviate commands and parameters as long as they contain enough letters to differentiate them from any other currently available commands or parameters. You can use the Tab key to complete partial commands, or enter a partial command followed by the “?” character to display a list of possible matches. You can also use the following editing keystrokes for command-line processing:

Table 5: Keystroke Commands

Keystroke	Function
Ctrl-A	Shifts cursor to start of command line.
Ctrl-B	Shifts cursor to the left one character.
Ctrl-C	Terminates the current task and displays the command prompt.
Ctrl-E	Shifts cursor to end of command line.
Ctrl-F	Shifts cursor to the right one character.
Ctrl-K	Deletes all characters from the cursor to the end of the line.
Ctrl-L	Repeats current command line on a new line.
Ctrl-N	Enters the next command line in the history buffer.
Ctrl-P	Enters the last command.
Ctrl-R	Repeats current command line on a new line.
Ctrl-U	Deletes from the cursor to the beginning of the line.
Ctrl-W	Deletes the last word typed.
Esc-B	Moves the cursor back one word.
Esc-D	Deletes from the cursor to the end of the word.
Esc-F	Moves the cursor forward one word.
Delete key or backspace key	Erases a mistake when entering a command.

CLI Command Groups

The system commands can be broken down into the functional groups shown below.

Table 6: Command Group Index

Command Group	Description	Page
General	Basic commands for entering privileged access mode, restarting the system, or quitting the CLI	93
System Management	Display and setting of system information, basic modes of operation, maximum frame size, file management, console port and telnet settings, system logs, SMTP alerts, the system clock, and switch clustering	101
Simple Network Management Protocol	Activates authentication failure traps; configures community access strings, and trap receivers	179
Remote Monitoring	Supports statistics, history, alarm and event groups	201
Flow Sampling	Samples traffic flows, and forwards data to designated collector	209
User Authentication	Configures user names and passwords, logon access using local or remote authentication, management access through the web server, Telnet server and Secure Shell; as well as port security, IEEE 802.1X port access control, restricted access based on specified IP addresses, and PPPoE Intermediate Agent	217
General Security Measures	Segregates traffic for clients attached to common data ports; and prevents unauthorized access by configuring valid static or dynamic addresses, web authentication, MAC address authentication, filtering DHCP requests and replies, and discarding invalid ARP responses	275
Access Control List	Provides filtering for IPv4 frames (based on address, protocol, TCP/UDP port number or TCP control code), IPv6 frames (based on address, or non-IP frames (based on MAC address or Ethernet type)	347
Interface	Configures the connection parameters for all Ethernet ports, aggregated links, and VLANs	369
Link Aggregation	Statically groups multiple ports into a single logical trunk; configures Link Aggregation Control Protocol for port trunks	401
Mirror Port	Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port	415
Congestion Control	Sets the input/output rate limits, traffic storm thresholds, and thresholds for broadcast and multicast storms which can be used to trigger configured rate limits or to shut down a port.	425
Address Table	Configures the address table for filtering specified addresses, displays current entries, clears the table, or sets the aging time	443
Spanning Tree	Configures Spanning Tree settings for the switch	449
VLANs	Configures VLAN settings, and defines port membership for VLAN groups; also enables or configures private VLANs, protocol VLANs, voice VLANs, and QinQ tunneling	477

Table 6: Command Group Index (Continued)

Command Group	Description	Page
Class of Service	Sets port priority for untagged frames, selects strict priority or weighted round robin, relative weight for each priority queue, also sets priority for TCP/UDP traffic types, IP precedence, and DSCP	527
Quality of Service	Configures Differentiated Services	547
Multicast Filtering	Configures IGMP multicast filtering, query, profile, and proxy parameters; specifies ports attached to a multicast router; also configures multicast VLAN registration, and IPv6 MLD snooping	591
Link Layer Discovery Protocol	Configures LLDP settings to enable information discovery about neighbor devices	695
Domain Name Service	Configures DNS services.	721
Dynamic Host Configuration Protocol	Configures DHCP client, relay and server functions	729
Router Redundancy	Configures router redundancy to create primary and backup routers	801
IP Interface	Configures IP address for the switch interfaces; also configures ARP parameters	749
IP Routing	Configures static unicast routing, policy-based unicast routing for BGP, and dynamic unicast routing	811
Multicast Routing	Configures multicast routing protocols PIM-DM and PIM-SM for IPv4 and IPv6	1011
Data Center	Configures Database Center Bridging Exchange (DCBX), Congestion Notification (CN), Enhanced Transmission Selection (ETS), and Priority-Based Flow Control (PFC)	565
Debug	Displays debugging information for all key functions These commands are not described in this manual. Please refer to the prompt messages included in the CLI interface.	

The access mode shown in the following tables is indicated by these abbreviations:

ACL (Access Control List Configuration)

CM (Class Map Configuration)

DC (DHCP Server Configuration)

GC (Global Configuration)

IC (Interface Configuration)

IPC (IGMP Profile Configuration)

LC (Line Configuration)

MST (Multiple Spanning Tree)

NE (Normal Exec)

PE (Privileged Exec)

PM (Policy Map Configuration)

RC (Router Configuration)

RM (Route Map Configuration)

VC (VLAN Database Configuration)

3

General Commands

The general commands are used to control the command access mode, configuration mode, and other basic functions.

Table 7: General Commands

Command	Function	Mode
<code>prompt</code>	Customizes the CLI prompt	GC
<code>reload</code>	Restarts the system at a specified time, after a specified delay, or at a periodic interval	GC
<code>enable</code>	Activates privileged mode	NE
<code>quit</code>	Exits a CLI session	NE, PE
<code>show history</code>	Shows the command history buffer	NE, PE
<code>configure</code>	Activates global configuration mode	PE
<code>disable</code>	Returns to normal mode from privileged mode	PE
<code>reload</code>	Restarts the system immediately	PE
<code>show reload</code>	Displays the current reload settings, and the time at which next scheduled reload will take place	PE
<code>end</code>	Returns to Privileged Exec mode	any config. mode
<code>exit</code>	Returns to the previous configuration mode, or exits the CLI	any mode
<code>help</code>	Shows how to use help	any mode
<code>?</code>	Shows options for command completion (context sensitive)	any mode

prompt This command customizes the CLI prompt. Use the **no** form to restore the default prompt.

Syntax

prompt *string*

no prompt

string - Any alphanumeric string to use for the CLI prompt.
(Maximum length: 255 characters)

Default Setting

Console

Command Mode

Global Configuration

Example

```
Console(config)#prompt RD2
RD2(config)#
```

reload (Global Configuration)

This command restarts the system at a specified time, after a specified delay, or at a periodic interval. You can reboot the system immediately, or you can configure the switch to reset after a specified amount of time. Use the **cancel** option to remove a configured setting.

Syntax

reload {**at** *hour minute* [{*month day* | *day month*} [*year*]] |
in {*hour hours* | **minute** *minutes* | **hour** *hours* **minute** *minutes*} |
regularity *hour minute* [**period** {**daily** | **weekly** *day-of-week* | **monthly** *day*}] |
cancel [**at** | **in** | **regularity**]

reload at - A specified time at which to reload the switch.

hour - The hour at which to reload. (Range: 0-23)

minute - The minute at which to reload. (Range: 0-59)

month - The month at which to reload. (january ... december)

day - The day of the month at which to reload. (Range: 1-31)

year - The year at which to reload. (Range: 1970-2037)

reload in - An interval after which to reload the switch.

hours - The number of hours, combined with the minutes, before the switch resets. (Range: 0-576)

minutes - The number of minutes, combined with the hours, before the switch resets. (Range: 0-59)

reload regularity - A periodic interval at which to reload the switch.

hour - The hour at which to reload. (Range: 0-23)

minute - The minute at which to reload. (Range: 0-59)

day-of-week - Day of the week at which to reload.
 (Range: monday ... saturday)

day - Day of the month at which to reload. (Range: 1-31)

reload cancel - Cancels the specified reload option.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ This command resets the entire system.
- ◆ Any combination of reload options may be specified. If the same option is re-specified, the previous setting will be overwritten.
- ◆ When the system is restarted, it will always run the Power-On Self-Test. It will also retain all configuration information stored in non-volatile memory by the [copy running-config startup-config](#) command (See [“copy” on page 125](#)).

Example

This example shows how to reset the switch after 30 minutes:

```

Console(config)#reload in minute 30
***
*** --- Rebooting at January  1 02:10:43 2013 ---
***

Are you sure to reboot the system at the specified time? <y/n>

```

enable This command activates Privileged Exec mode. In privileged mode, additional commands are available, and certain commands display additional information. See [“Understanding Command Modes” on page 86](#).

Syntax

enable [*level*]

level - Privilege level to log into the device.

The device has two predefined privilege levels: 0: Normal Exec, 15: Privileged Exec. Enter level 15 to access Privileged Exec mode.

Default Setting

Level 15

Command Mode

Normal Exec

Command Usage

- ◆ “super” is the default password required to change the command mode from Normal Exec to Privileged Exec. (To set this password, see the [enable password](#) command.)
- ◆ The “#” character is appended to the end of the prompt to indicate that the system is in privileged access mode.

Example

```
Console>enable
Password: [privileged level password]
Console#
```

Related Commands

[disable \(98\)](#)

[enable password \(218\)](#)

quit This command exits the configuration program.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The **quit** and **exit** commands can both exit the configuration program.

Example

This example shows how to quit a CLI session:

```
Console#quit

Press ENTER to start session

User Access Verification

Username:
```

show history This command shows the contents of the command history buffer.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The history buffer size is fixed at 10 Execution commands and 10 Configuration commands.

Example

In this example, the show history command lists the contents of the command history buffer:

```

Console#show history
Execution command history:
 2 config
 1 show history

Configuration command history:
 4 interface vlan 1
 3 exit
 2 interface vlan 1
 1 end

Console#

```

The **!** command repeats commands from the Execution command history buffer when you are in Normal Exec or Privileged Exec Mode, and commands from the Configuration command history buffer when you are in any of the configuration modes. In this example, the **!2** command repeats the second command in the Execution history buffer (**config**).

```

Console#!2
Console#config
Console(config)#

```

configure This command activates Global Configuration mode. You must enter this mode to modify any settings on the switch. You must also enter Global Configuration mode prior to enabling some of the other configuration modes, such as Interface Configuration, Line Configuration, and VLAN Database Configuration. See ["Understanding Command Modes" on page 86](#).

Default Setting

None

Command Mode

Privileged Exec

Example

```

Console#configure
Console(config)#

```

Related Commands

[end \(99\)](#)

disable This command returns to Normal Exec mode from privileged mode. In normal access mode, you can only display basic information on the switch's configuration or Ethernet statistics. To gain access to all commands, you must use the privileged mode. See [“Understanding Command Modes” on page 86](#).

Default Setting

None

Command Mode

Privileged Exec

Command Usage

The “>” character is appended to the end of the prompt to indicate that the system is in normal access mode.

Example

```
Console#disable
Console>
```

Related Commands

[enable \(95\)](#)

reload This command restarts the system.
(Privileged Exec)



Note: When the system is restarted, it will always run the Power-On Self-Test. It will also retain all configuration information stored in non-volatile memory by the copy running-config startup-config command.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

This command resets the entire system.

Example

This example shows how to reset the switch:

```
Console#reload
System will be restarted, continue <y/n>? y
```

show reload This command displays the current reload settings, and the time at which next scheduled reload will take place.

Command Mode

Privileged Exec

Example

```
Console#show reload
Reloading switch in time:                0 hours 29 minutes.

The switch will be rebooted at January  1 02:11:50 2001.
Remaining Time: 0 days, 0 hours, 29 minutes, 52 seconds.
Console#
```

end This command returns to Privileged Exec mode.

Default Setting

None

Command Mode

Global Configuration, Interface Configuration, Line Configuration, VLAN Database Configuration, and Multiple Spanning Tree Configuration.

Example

This example shows how to return to the Privileged Exec mode from the Interface Configuration mode:

```
Console(config-if)#end
Console#
```

exit This command returns to the previous configuration mode or exits the configuration program.

Default Setting

None

Command Mode

Any

Example

This example shows how to return to the Privileged Exec mode from the Global Configuration mode, and then quit the CLI session:

```
Console(config)#exit
Console#exit

Press ENTER to start session

User Access Verification

Username:
```

4

System Management Commands

The system management commands are used to control system logs, passwords, user names, management options, and display or configure a variety of other system information.

Table 8: System Management Commands

Command Group	Function
Device Designation	Configures information that uniquely identifies this switch
Banner Information	Configures administrative contact, device identification and location
System Status	Displays system configuration, active managers, and version information
Fan Control	Forces fans to full speed
Frame Size	Enables support for jumbo frames
File Management	Manages code image or switch configuration files
Line	Sets communication parameters for the serial port, including baud rate and console time-out
Event Logging	Controls logging of error messages
SMTP Alerts	Configures SMTP email alerts
Time (System Clock)	Sets the system clock automatically via NTP/SNTP server or manually
Time Range	Sets a time range for use by other functions, such as Access Control Lists
Switch Clustering	Configures management of multiple devices via a single IP address

Device Designation

This section describes commands used to configure information that uniquely identifies the switch.

Table 9: Device Designation Commands

Command	Function	Mode
hostname	Specifies the host name for the switch	GC
snmp-server contact	Sets the system contact string	GC
snmp-server location	Sets the system location string	GC

hostname This command specifies or modifies the host name for this device. Use the **no** form to restore the default host name.

Syntax

hostname *name*

no hostname

name - The name of this host. (Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#hostname RD#1
Console(config)#
```

Banner Information

These commands are used to configure and manage administrative information about the switch, its exact data center location, details of the electrical and network circuits that supply the switch, as well as contact information for the network administrator and system manager. This information is only available via the CLI and is automatically displayed before login as soon as a console or telnet connection has been established.

Table 10: Banner Commands

Command	Function	Mode
<code>banner configure</code>	Configures the banner information that is displayed before login	GC
<code>banner configure company</code>	Configures the Company information that is displayed by banner	GC
<code>banner configure dc-power-info</code>	Configures the DC Power information that is displayed by banner	GC
<code>banner configure department</code>	Configures the Department information that is displayed by banner	GC
<code>banner configure equipment-info</code>	Configures the Equipment information that is displayed by banner	GC
<code>banner configure equipment-location</code>	Configures the Equipment Location information that is displayed by banner	GC
<code>banner configure ip-lan</code>	Configures the IP and LAN information that is displayed by banner	GC

Table 10: Banner Commands (Continued)

Command	Function	Mode
<code>banner configure lp-number</code>	Configures the LP Number information that is displayed by banner	GC
<code>banner configure manager-info</code>	Configures the Manager contact information that is displayed by banner	GC
<code>banner configure mux</code>	Configures the MUX information that is displayed by banner	GC
<code>banner configure note</code>	Configures miscellaneous information that is displayed by banner under the Notes heading	GC
<code>show banner</code>	Displays all banner information	NE, PE

banner configure This command is used to interactively specify administrative information for this device.

Syntax

banner configure

Default Setting

None

Command Mode

Global Configuration

Command Usage

The administrator can batch-input all details for the switch with one command. When the administrator finishes typing the company name and presses the enter key, the script prompts for the next piece of information, and so on, until all information has been entered. Pressing enter without inputting information at any prompt during the script's operation will leave the field empty. Spaces can be used during script mode because pressing the enter key signifies the end of data input. The delete and left-arrow keys terminate the script. The use of the backspace key during script mode is not supported. If, for example, a mistake is made in the company name, it can be corrected with the **banner configure company** command.

Example

```
Console(config)#banner configure
```

```
Company: Edgecore Networks
Responsible department: R&D Dept
Name and telephone to Contact the management people
Manager1 name: Sr. Network Admin
  phone number: 123-555-1212
Manager2 name: Jr. Network Admin
  phone number: 123-555-1213
Manager3 name: Night-shift Net Admin / Janitor
  phone number: 123-555-1214
```

```
The physical location of the equipment.  
City and street address: 12 Straight St. Motown, Zimbabwe  
Information about this equipment:  
Manufacturer: Edge-Core Networks  
ID: 123_unique_id_number  
Floor: 2  
Row: 7  
Rack: 29  
Shelf in this rack: 8  
Information about DC power supply.  
Floor: 2  
Row: 7  
Rack: 25  
Electrical circuit: : ec-177743209-xb  
Number of LP:12  
Position of the equipment in the MUX:1/23  
IP LAN:192.168.1.1  
Note: This is a random note about this managed switch and can contain  
      miscellaneous information.  
Console(config)#
```

banner configure company This command is used to configure company information displayed in the banner. Use the **no** form to remove the company name from the banner display.

Syntax

banner configure company *name*

no banner configure company

name - The name of the company. (Maximum length: 32 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

Input strings cannot contain spaces. The **banner configure company** command interprets spaces as data input boundaries. The use of underscores (`_`) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

Example

```
Console(config)#banner configure company Big-Ben  
Console(config)#
```


banner configure dc-power-info This command is use to configure DC power information displayed in the banner. Use the **no** form to restore the default setting.

Syntax

banner configure dc-power-info floor *floor-id* **row** *row-id* **rack** *rack-id*
electrical-circuit *ec-id*

no banner configure dc-power-info [**floor** | **row** | **rack** | **electrical-circuit**]

floor-id - The floor number.

row-id - The row number.

rack-id - The rack number.

ec-id - The electrical circuit ID.

Maximum length of each parameter: 32 characters

Default Setting

None

Command Mode

Global Configuration

Command Usage

Input strings cannot contain spaces. The **banner configure dc-power-info** command interprets spaces as data input boundaries. The use of underscores (`_`) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

Example

```
Console(config)#banner configure dc-power-info floor 3 row 15 rack 24  
electrical-circuit 48v-id_3.15.24.2  
Console(config)#
```

banner configure department This command is used to configure the department information displayed in the banner. Use the **no** form to restore the default setting.

Syntax

banner configure department *dept-name*

no banner configure department

dept-name - The name of the department.
(Maximum length: 32 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

Input strings cannot contain spaces. The **banner configure department** command interprets spaces as data input boundaries. The use of underscores (`_`) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

Example

```
Console(config)#banner configure department R&D
Console(config)#
```

banner configure equipment-info This command is used to configure the equipment information displayed in the banner. Use the **no** form to restore the default setting.

Syntax

banner configure equipment-info manufacturer-id *mfr-id* **floor** *floor-id*
row *row-id* **rack** *rack-id* **shelf-rack** *sr-id* **manufacturer** *mfr-name*

no banner configure equipment-info [**floor** | **manufacturer** | **manufacturer-id** | **rack** | **row** | **shelf-rack**]

mfr-id - The name of the device model number.

floor-id - The floor number.

row-id - The row number.

rack-id - The rack number.

sr-id - The shelf number in the rack.

mfr-name - The name of the device manufacturer.

Maximum length of each parameter: 32 characters

Default Setting

None

Command Mode

Global Configuration

Command Usage

Input strings cannot contain spaces. The **banner configure equipment-info** command interprets spaces as data input boundaries. The use of underscores (`_`) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

Example

```
Console(config)#banner configure equipment-info manufacturer-id ECS4660-28F  
floor 3 row 10 rack 15 shelf-rack 12 manufacturer Edge-Core  
Console(config)#
```

banner configure equipment-location This command is used to configure the equipment location information displayed in the banner. Use the **no** form to restore the default setting.

Syntax

banner configure equipment-location *location*

no banner configure equipment-location

location - The address location of the device.
(Maximum length: 32 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

Input strings cannot contain spaces. The **banner configure equipment-location** command interprets spaces as data input boundaries. The use of underscores (`_`) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

Example

```
Console(config)#banner configure equipment-location  
710_Network_Path,_Indianapolis  
Console(config)#
```

banner configure ip-lan This command is used to configure the device IP address and subnet mask information displayed in the banner. Use the **no** form to restore the default setting.

Syntax

banner configure ip-lan *ip-mask*

no banner configure ip-lan

ip-mask - The IP address and subnet mask of the device.
(Maximum length: 32 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

Input strings cannot contain spaces. The **banner configure ip-lan** command interprets spaces as data input boundaries. The use of underscores (`_`) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

Example

```
Console(config)#banner configure ip-lan 192.168.1.1/255.255.255.0
Console(config)#
```

banner configure lp-number This command is used to configure the LP number information displayed in the banner. Use the **no** form to restore the default setting.

Syntax

banner configure lp-number *lp-num*

no banner configure lp-number

lp-num - The LP number. (Maximum length: 32 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

Input strings cannot contain spaces. The **banner configure lp-number** command interprets spaces as data input boundaries. The use of underscores (`_`) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

Example

```
Console(config)#banner configure lp-number 12
Console(config)#
```

banner configure manager-info This command is used to configure the manager contact information displayed in the banner. Use the **no** form to restore the default setting.

Syntax

banner configure manager-info

name *mgr1-name* **phone-number** *mgr1-number*
[name2 *mgr2-name* **phone-number** *mgr2-number* |
name3 *mgr3-name* **phone-number** *mgr3-number*]

no banner configure manager-info [**name1** | **name2** | **name3**]

mgr1-name - The name of the first manager.

mgr1-number - The phone number of the first manager.

mgr2-name - The name of the second manager.

mgr2-number - The phone number of the second manager.

mgr3-name - The name of the third manager.

mgr3-number - The phone number of the third manager.

Maximum length of each parameter: 32 characters

Default Setting

None

Command Mode

Global Configuration

Command Usage

Input strings cannot contain spaces. The **banner configure manager-info** command interprets spaces as data input boundaries. The use of underscores (`_`) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

Example

```
Console(config)#banner configure manager-info name Albert_Einstein phone-  
number 123-555-1212 name2 Lamar phone-number 123-555-1219  
Console(config)#
```

banner configure mux This command is used to configure the mux information displayed in the banner. Use the **no** form to restore the default setting.

Syntax

banner configure mux *muxinfo*

no banner configure mux

muxinfo - The circuit and PVC to which the switch is connected. (Maximum length: 32 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

Input strings cannot contain spaces. The **banner configure mux** command interprets spaces as data input boundaries. The use of underscores (`_`) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

Example

```
Console(config)#banner configure mux telco-8734212kx_PVC-1/23
Console(config)#
```

banner configure note This command is used to configure the note displayed in the banner. Use the **no** form to restore the default setting.

Syntax

banner configure note *note-info*

no banner configure note

note-info - Miscellaneous information that does not fit the other banner categories, or any other information of importance to users of the switch CLI. (Maximum length: 150 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

Input strings cannot contain spaces. The **banner configure note** command interprets spaces as data input boundaries. The use of underscores (`_`) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

Example

```
Console(config)#banner configure note !!!!!ROUTINE_MAINTENANCE_firmware-
upgrade_0100-0500_GMT-0500_20071022!!!!_20min_network_impact_expected
Console(config)#
```

show banner This command displays all banner information.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show banner
Edge-Core
WARNING - MONITORED ACTIONS AND ACCESSES
R&D

Albert_Einstein - 123-555-1212
Lamar - 123-555-1219

Station's information:
710_Network_Path,_Indianapolis

Edge-Core - ECS4660-28F
Floor / Row / Rack / Sub-Rack
3/ 10 / 15 / 12
DC power supply:
Power Source A: Floor / Row / Rack / Electrical circuit
3/ 15 / 24 / 48v-id_3.15.24.2
Number of LP: 12
Position MUX: telco-8734212kx_PVC-1/23
IP LAN: 192.168.1.1/255.255.255.0
Note: !!!!!ROUTINE_MAINTENANCE_firmware-upgrade_0100-0500_GMT-
0500_20071022!!!!!!_20min_network_
Console#
```

System Status

This section describes commands used to display system information.

Table 11: System Status Commands

Command	Function	Mode
location-led	Flashes the Locator LED to indicate the unit to which you are connected	PE
show access-list tcam-utilization	Shows utilization parameters for TCAM	PE
show location-led status	Shows if location LED function is enabled or not	PE
show memory	Shows memory utilization parameters	NE, PE
show process cpu	Shows CPU utilization parameters	NE, PE
show running-config	Displays the configuration data currently in use	PE
show startup-config	Displays the contents of the configuration file (stored in flash memory) that is used to start up the system	PE
show system	Displays system information	NE, PE

Table 11: System Status Commands (Continued)

Command	Function	Mode
<code>show tech-support</code>	Displays a detailed list of system settings designed to help technical support resolve configuration or functional problems	PE
<code>show users</code>	Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet clients	NE, PE
<code>show version</code>	Displays version information for the system	NE, PE
<code>show watchdog</code>	Shows if watchdog debugging is enabled	PE
<code>watchdog software</code>	Monitors key processes, and automatically reboots the system if any of these processes are not responding correctly	PE

location-led This command flashes the Locator LED to indicate the unit to which you are connected.

Syntax

location-led {on | off}

Command Mode

Privileged Exec

Command Usage

The Locator LED is labeled “Loc.” It is located in the upper right corner of the front panel.

Example

```
Console#location-led on
Console#
```

show access-list tcam-utilization This command shows utilization parameters for TCAM (Ternary Content Addressable Memory), including the number policy control entries in use, the number of free entries, and the overall percentage of TCAM in use.

Command Mode

Privileged Exec

Command Usage

Policy control entries (PCEs) are used by various system functions which rely on rule-based searches, including Access Control Lists (ACLs), IP Source Guard filter rules, Quality of Service (QoS) processes, or traps.

For example, when binding an ACL to a port, each rule in an ACL will use two PCEs; and when setting an IP Source Guard filter rule for a port, the system will also use two PCEs.

Example

```
Console#show access-list tcam-utilization
Total Policy Control Entries : 960
Free Policy Control Entries  : 960
Entries Used by System      : 0
Entries Used by User        : 0
TCAM Utilization            : 0.0%
Console#
```

show location-led status This command shows if location LED function is enabled or not.

Command Mode

Privileged Exec

Example

```
Console#show location-led status
Location Led Status:On
Console#
```

show memory This command shows memory utilization parameters, and alarm thresholds.

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command shows the amount of memory currently free for use, the amount of memory allocated to active processes, and the total amount of system memory.

Example

```
Console#show memory
Status Bytes      %
-----
Free    404119552  18
Used    1743364096 82
Total   2147483648

Alarm Configuration
Rising Threshold      : 90%
Falling Threshold     : 70%

Console#
```

Related Commands

[memory \(198\)](#)

show process cpu This command shows the CPU utilization parameters, alarm status, and alarm configuration.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show process cpu
CPU Utilization in the past 5 seconds : 7%

CPU Utilization in the past 60 seconds
Average Utilization      : 8%
Maximum Utilization      : 9%

Alarm Status
Current Alarm Status     : Off
Last Alarm Start Time    : Jun  9 15:10:09 2011
Last Alarm Duration Time : 10 seconds

Alarm Configuration
Rising Threshold         : 90%
Falling Threshold        : 70%

Console#
```

Related Commands

[process cpu \(198\)](#)

show running-config This command displays the configuration information currently in use.

Syntax

show running-config

Command Mode

Privileged Exec

Command Usage

- ◆ Use this command in conjunction with the **show startup-config** command to compare the information in running memory to the information stored in non-volatile memory.
- ◆ This command displays settings for key command modes. Each mode group is separated by “!” symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:
 - MAC address for the switch
 - SNMP community strings
 - Users (names, access levels, and encrypted passwords)
 - VLAN database (VLAN ID, name and state)
 - VLAN configuration settings for each interface

- Multiple spanning tree instances (name and interfaces)
- IP address configured for management VLAN
- Interface settings
- Any configured settings for the console port and Telnet

Example

```

Console#show running-config
Building startup configuration. Please wait...
!<stackingDB>00</stackingDB>
!<stackingMac>01_00-e0-0c-00-00-fd_00</stackingMac>
!
snmp-server community public ro
snmp-server community private rw
!
snmp-server enable traps authentication
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
vlan database
VLAN 1 name DefaultVlan media ethernet state active
!
spanning-tree mst configuration
!
interface ethernet 1/1
no negotiation
:
!
interface ethernet 1/1
switchport allowed vlan add 1 untagged
switchport native vlan 1
switchport allowed vlan add 4093 tagged
:
!
control-plane
!
interface vlan 1
ip address dhcp
!
interface craft
!
line console
!
line vty
!
end
!
Console#

```

Related Commands

[show startup-config \(116\)](#)

show startup-config This command displays the configuration file stored in non-volatile memory that is used to start up the system.

Command Mode

Privileged Exec

Command Usage

- ◆ Use this command in conjunction with the **show running-config** command to compare the information in running memory to the information stored in non-volatile memory.
- ◆ This command displays settings for key command modes. Each mode group is separated by “!” symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:
 - MAC address for the switch
 - SNMP community strings
 - Users (names, access levels, and encrypted passwords)
 - VLAN database (VLAN ID, name and state)
 - VLAN configuration settings for each interface
 - Multiple spanning tree instances (name and interfaces)
 - IP address configured for management VLAN
 - Interface settings
 - Any configured settings for the console port and Telnet

Example

Refer to the example for the running configuration file.

Related Commands

[show running-config \(114\)](#)

show system This command displays system information.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

- ◆ There is one fan tray in the switch. The tray includes four fixed fans and supports manual fan speed control using the [fan-speed force-full](#) command. These fans provide cooling for the internal components using front-to-back or back-to-front airflow. (Note that the power supply units include built-in fans.)
- ◆ There are two thermal detectors in the switch. The first detector is near the air flow intake vents. The second detector is near the switch ASIC and CPU.

Example

```

Console#show system
System Description : ECS5610-52S
System OID String : 1.3.6.1.4.1.259.10.1.36.101
System Information
  System Up Time      : 0 days, 5 hours, 44 minutes, and 42.28 seconds
  System Name         :
  System Location     :
  System Contact      :
  MAC Address (Unit 1) : 00-00-0C-00-00-FD
  Web Server          : Enabled
  Web Server Port     : 80
  Web Secure Server   : Enabled
  Web Secure Server Port : 443
  Telnet Server       : Enabled
  Telnet Server Port  : 23
  Jumbo Frame        : Disabled

System Fan:
  Force Fan Speed Full : Disabled
Unit 1
  Fan 1: Ok

System Temperature:
Unit 1
  Temperature 1: 39 degrees      Temperature 2: 37 degrees
  Temperature 3: 38 degrees      Temperature 4: 31 degrees
  Temperature 5: 31 degrees      Temperature 6: 29 degrees
  Temperature 7: 29 degrees      Temperature 8: 36 degrees
  Temperature 9: 36 degrees

Main Power Status      : Up
Redundant Power Status : Not present
Console#

```

Table 12: show system – display description

Parameter	Description
System Description	Brief description of device type.
System Object ID	MIB II object ID for switch's network management subsystem.
System Up Time	Length of time the management agent has been up.
System Name	Name assigned to the switch system.
System Location	Specifies the system location.
System Contact	Administrator responsible for the system.
MAC Address	MAC address assigned to this switch.
Web Server/Port	Shows administrative status of web server and UDP port number.
Web Secure Server/Port	Shows administrative status of secure web server and UDP port number.
Telnet Server/Port	Shows administrative status of Telnet server and TCP port number.
Jumbo Frame	Shows if jumbo frames are enabled or disabled.
System Fan	Shows if forced full-speed mode is enabled.

Table 12: show system – display description (Continued)

Parameter	Description
System Temperature	Temperature at specified thermal detection point.
Main Power Status	Displays the status of the internal power supply.
Redundant Power Status	Displays the status of the redundant power supply. (This switch does not support a redundant power supply.)

show tech-support This command displays a detailed list of system settings designed to help technical support resolve configuration or functional problems.

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command generates a long list of information including detailed system and interface settings. It is therefore advisable to direct the output to a file using any suitable output capture function provided with your terminal emulation program.

Example

```
Console#show tech-support

show system:
System Description : ECS5610-52S
System OID String  : 1.3.6.1.4.1.259.10.1.36.101
System Information
System Up Time:      0 days, 2 hours, 17 minutes, and 6.23 seconds
System Name:         [NONE]
System Location:     [NONE]
System Contact:      [NONE]
MAC Address (Unit1): 00-12-CF-61-24-2F
Web Server:          Enabled
Web Server Port:     80
Web Secure Server:   Enabled
Web Secure Server Port: 443
Telnet Server:        Enable
Telnet Server Port:  23
Jumbo Frame:         Disabled
:
```

show users Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet client.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The session used to execute this command is indicated by a "*" symbol next to the Line (i.e., session) index number.

Example

```

Console#show users
User Name Accounts:
  User Name                               Privilege Public-Key
  -----
  admin                                   15 None
  guest                                  0 None
  steve                                  15 RSA

Online Users:
  Line    User Name                               Idle time (h:m:s) Remote IP addr
  -----
  *console admin                               0:14:14
  VTY 0    admin                               0:00:00    192.168.1.19
  SSH 1    steve                               0:00:06    192.168.1.19

Web Online Users:
  Line    User Name                               Idle time (h:m:s) Remote IP Addr
  -----
  HTTP    admin                               0:00:06 192.168.0.99

Console#

```

show version This command displays hardware and software version information for the system.

Command Mode

Normal Exec, Privileged Exec

Example

```

Console#show version
Unit 1
  Serial Number      : S123456
  Hardware Version   : R0A
  EPLD Version       : 0.02
  Number of Ports    : 52
  Main Power Status  : Not present
  Redundant Power Status : Up
  Role               : Master
  Loader Version     : 0.0.0.2
  Linux Kernel Version : 2.6.32
  Boot ROM Version    : 1.0.0.1
  Operation Code Version : 1.0.0.0

Console#

```

Table 13: show version – display description

Parameter	Description
Serial Number	The serial number of the switch.
Hardware Version	Hardware version of the main board.
EPLD Version	Version number of Erasable Programmable Logic Device.
Number of Ports	Number of built-in ports.
Main Power Status	Displays the status of the internal power supply.
Redundant Power Status	Displays the status of the redundant power supply. (This switch does not support a redundant power supply.)
Role	Shows that this switch is operating as Master or Slave.
Loader Version	Version number of loader code.
Linux Kernel Version	Version number of Linux kernel.
Boot ROM Version	Version of Power-On Self-Test (POST) and boot code.
Operation Code Version	Version number of runtime code.

show watchdog This command shows if watchdog debugging is enabled.

Command Mode
Privileged Exec

Example

```
Console#show watchdog

Software Watchdog Information
Status :    Enabled
Console#
```

watchdog software This command monitors key processes, and automatically reboots the system if any of these processes are not responding correctly.

Syntax

watchdog software {disable | enable}

Default Setting
Disabled

Command Mode
Privileged Exec

Example

```
Console#watchdog
Console#
```

Fan Control

This section describes the command used to force fan speed.

Table 14: Fan Control Commands

Command	Function	Mode
<code>fan-speed force-full</code>	Forces fans to full speed	GC
<code>show system</code>	Shows if full fan speed is enabled	NE, PE

fan-speed force-full This command sets all fans to full speed. Use the `no` form to reset the fans to normal operating speed.

Syntax

[no] fan-speed force-full

Default Setting

Normal speed

Command Mode

Global Configuration

Example

```
Console(config)#fan-speed force-full
Console(config)#
```

Frame Size

This section describes commands used to configure the Ethernet frame size on the switch.

Table 15: Frame Size Commands

Command	Function	Mode
<code>jumbo frame</code>	Enables support for jumbo frames	GC

jumbo frame This command enables support for layer 2 jumbo frames for Gigabit and 10 Gigabit Ethernet ports. Use the **no** form to disable it.

Syntax

[no] jumbo frame

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ This switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames on Gigabit and 10 Gigabit Ethernet ports or trunks of up to 12288 bytes. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.
- ◆ To use jumbo frames, both the source and destination end nodes (such as a computer or server) must support this feature. Also, when the connection is operating at full duplex, all switches in the network between the two end nodes must be able to accept the extended frame size. And for half-duplex connections, all devices in the collision domain would need to support jumbo frames.
- ◆ This command globally enables support for jumbo frames on all Gigabit and 10 Gigabit ports and trunks. To set the MTU for a specific interface, enable jumbo frames and use the [switchport mtu](#) command to specify the required size of the MTU.
- ◆ The current setting for jumbo frames can be displayed with the [show system](#) command.

Example

```
Console(config)#jumbo frame
Console(config)#
```

File Management

Managing Firmware

Firmware can be uploaded and downloaded to or from an FTP/TFTP server or through the USB port. By saving runtime code to a file on an FTP/TFTP server, that file can later be downloaded to the switch to restore operation. The switch can also be set to use new firmware without overwriting the previous version.

When downloading runtime code, the destination file name can be specified to replace the current image, or the file can be first downloaded using a different name from the current runtime code file, and then the new file set as the startup file.

Saving or Restoring Configuration Settings

Configuration settings can be uploaded and downloaded to and from an FTP/TFTP server. The configuration file can be later downloaded to restore switch settings.

The configuration file can be downloaded under a new file name and then set as the startup file, or the current startup configuration file can be specified as the destination file to directly replace it. Note that the file "Factory_Default_Config.cfg" can be copied to the FTP/TFTP server, but cannot be used as the destination on the switch.

Table 16: Flash/File Commands

Command	Function	Mode
<i>General Commands</i>		
<code>boot system</code>	Specifies the file or image used to start up the system	GC
<code>copy</code>	Copies a code image or a switch configuration to or from flash memory or an FTP/TFTP server	PE
<code>delete</code>	Deletes a file or code image	PE
<code>dir</code>	Displays a list of files in flash memory	PE
<code>umount usbdisk</code>	Prepares the USB memory device to be safely removed	PE
<code>whichboot</code>	Displays the files booted	PE
<i>Automatic Code Upgrade Commands</i>		
<code>upgrade opcode auto</code>	Automatically upgrades the current image when a new version is detected on the indicated server	GC
<code>upgrade opcode path</code>	Specifies an FTP/TFTP server and directory in which the new opcode is stored	GC
<code>upgrade opcode reload</code>	Reloads the switch automatically after the opcode upgrade is completed	GC
<code>show upgrade</code>	Shows the opcode upgrade configuration settings.	PE

General Commands

boot system This command specifies the file or image used to start up the system.

Syntax

boot system {**boot-rom** | **config** | **opcode**}; *filename*

boot-rom* - Boot ROM.

config* - Configuration file.

opcode* - Run-time operation code.

filename - Name of configuration file or code image.

* The colon (:) is required.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ A colon (:) is required after the specified file type.
- ◆ If the file contains an error, it cannot be set as the default file.

Example

```
Console(config)#boot system config: startup
Console(config)#
```

Related Commands

[dir \(129\)](#)

[whichboot \(130\)](#)

copy This command moves (upload/download) a code image or configuration file between the switch's flash memory and an FTP/TFTP server or a USB memory stick. When you save the system code or configuration settings to a file on an FTP/TFTP server, that file can later be downloaded to the switch to restore system operation. The success of the file transfer depends on the accessibility of the FTP/TFTP server and the quality of the network connection.

Syntax

```
copy file {file | ftp | running-config | startup-config | tftp}  
copy ftp {add-to-running-config | file | https-certificate | public-key |  
running-config | startup-config}  
copy running-config {file | ftp | startup-config | tftp}  
copy startup-config {file | ftp | running-config | tftp}  
copy tftp {add-to-running-config | file | https-certificate | public-key |  
running-config | startup-config}  
copy usbdisk file
```

add-to-running-config - Keyword that adds the settings listed in the specified file to the running configuration.

file - Keyword that allows you to copy to/from a file.

ftp - Keyword that allows you to copy to/from an FTP server.

https-certificate - Keyword that allows you to copy the HTTPS secure site certificate.

public-key - Keyword that allows you to copy a SSH key from a TFTP server. (See "Secure Shell" on page 243.)

running-config - Keyword that allows you to copy to/from the current running configuration.

startup-config - The configuration used for system initialization.

tftp - Keyword that allows you to copy to/from a TFTP server.

usbdisk - Keyword that allows you to copy to/from a USB memory stick. (USB slot only supports simple data storage devices using a FAT16/32 file system with or without a partition table.)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- ◆ The system prompts for data required to complete the copy command.
- ◆ The destination file name should not contain slashes (\ or /), and the maximum length for file names is 32 characters for files on the switch or 128 characters for files on the server. (Valid characters: A-Z, a-z, 0-9, " ", "-")

- ◆ The switch supports only two operation code files, but the maximum number of user-defined configuration files is 16.
- ◆ You can use "Factory_Default_Config.cfg" as the source to copy from the factory default configuration file, but you cannot use it as the destination.
- ◆ To replace the startup configuration, you must use **startup-config** as the destination.
- ◆ The Boot ROM and Loader cannot be uploaded or downloaded from the FTP/TFTP server. You must follow the instructions in the release notes for new firmware, or contact your distributor for help.
- ◆ For information on specifying an https-certificate, see "Replacing the Default Secure-site Certificate" in the *Web Management Guide*. For information on configuring the switch to use HTTPS for a secure connection, see the `ip http secure-server` command.
- ◆ When logging into an FTP server, the interface prompts for a user name and password configured on the remote server. Note that "anonymous" is set as the default user name.

Example

The following example shows how to download new firmware from a TFTP server:

```
Console#copy tftp file
TFTP server ip address: 10.1.0.19
Choose file type:
  1. config:  2. opcode: 2
Source file name: m360.bix
Destination file name: m360.bix
\Write to FLASH Programming.
-Write to FLASH finish.
Success.
Console#
```

The following example shows how to upload the configuration settings to a file on the TFTP server:

```
Console#copy file tftp
Choose file type:
  1. config:  2. opcode: 1
Source file name: startup
TFTP server ip address: 10.1.0.99
Destination file name: startup.01
TFTP completed.
Success.

Console#
```

The following example shows how to copy the running configuration to a startup file.

```
Console#copy running-config file
destination file name: startup
Write to FLASH Programming.
\Write to FLASH finish.
Success.

Console#
```

The following example shows how to download a configuration file:

```
Console#copy tftp startup-config
TFTP server ip address: 10.1.0.99
Source configuration file name: startup.01
Startup configuration file name [startup]:
Write to FLASH Programming.

\Write to FLASH finish.
Success.

Console#
```

This example shows how to copy a secure-site certificate from an TFTP server. It then reboots the switch to activate the certificate:

```
Console#copy tftp https-certificate
TFTP server ip address: 10.1.0.19
Source certificate file name: SS-certificate
Source private file name: SS-private
Private password: *****

Success.
Console#reload
System will be restarted, continue <y/n>? y
```

This example shows how to copy a public-key used by SSH from an TFTP server. Note that public key authentication via SSH is only supported for users configured locally on the switch.

```
Console#copy tftp public-key
TFTP server IP address: 192.168.1.19
Choose public key type:
 1. RSA:  2. DSA: 1
Source file name: steve.pub
Username: steve
TFTP Download
Success.
Write to FLASH Programming.
Success.

Console#
```

This example shows how to copy a file to an FTP server.

```
Console#copy ftp file
FTP server IP address: 169.254.1.11
User[anonymous]: admin
Password[]: *****
Choose file type:
  1. config:  2. opcode: 2
Source file name: BLANC.BIX
Destination file name: BLANC.BIX
Console#
```

delete This command deletes a file or image.

Syntax

delete [**usbdisk**] *filename*

usbdisk - System file on a USB memory stick or disk.

filename - Name of configuration file or code image.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- ◆ If the file type is used for system startup, then this file cannot be deleted.
- ◆ "Factory_Default_Config.cfg" cannot be deleted.

Example

This example shows how to delete the test2.cfg configuration file from flash memory.

```
Console#delete test2.cfg
Console#
```

Related Commands

[dir \(129\)](#)

[delete public-key \(248\)](#)

dir This command displays a list of files in flash memory.

Syntax

dir {**boot-rom**: | **config**: | **opcode**: | **usbdisk**:} [*filename*]

boot-rom - Boot ROM (or diagnostic) image file.

config - Switch configuration file.

opcode - Run-time operation code image file.

usbdisk - System file on a USB memory stick or disk.

filename - Name of configuration file or code image. If this file exists but contains errors, information on this file cannot be shown.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- ◆ If you enter the command **dir** without any parameters, the system displays all files.

File information is shown below:

Table 17: File Directory Information

Column Heading	Description
File Name	The name of the file.
File Type	File types: Boot-Rom, Operation Code, and Config file.
Startup	Shows if this file is used when the system is started.
Create Time	The date and time the file was created.
Size	The length of the file in bytes.

Example

The following example shows how to display all file information:

```

Console#dir
      File Name                               Type  Startup Modify Time          Size(bytes)
-----
Unit 1:
ECS5610_52S_V0.1.0.0.bix                     OpCode   N    1970-01-01 00:00:48    24731245
ECS5610_52S_V1.2.2.1.bix                     OpCode   Y    2012-12-04 13:23:59    25783857
Factory_Default_Config.cfg                   Config   N    2012-12-04 13:18:37      455
startupl.cfg                                Config   Y    2012-12-04 13:18:44    3055
-----
Free space for compressed user config files:1594384384
Console#

```

umount usbdisk This command prepares the USB memory device to be safely removed from the switch.

Syntax

umount usbdisk

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Before disconnecting a USB memory device, you must unmount it first. This is similar to “Safely Remove Hardware” in Windows where the device will not unmount until all data transfers have been finished.

Example

```
Console#umount usbdisk
You can safely remove your usbdisk.
Console#
```

whichboot This command displays which files were booted when the system powered up.

Syntax

whichboot

Default Setting

None

Command Mode

Privileged Exec

Example

This example shows the information displayed by the **whichboot** command. See the table under the **dir** command for a description of the file information displayed by this command.

```
Console#whichboot
File Name                               Type  Startup Modify Time          Size(bytes)
-----
Unit 1:
ECS5610_52S_V1.2.2.1.bix               OpCode   Y    2012-12-04 13:23:59    25783857
startup1.cfg                           Config   Y    2012-12-04 13:18:44      3055
Console#
```

Automatic Code Upgrade Commands

upgrade opcode auto This command automatically upgrades the current operational code when a new version is detected on the server indicated by the [upgrade opcode path](#) command. Use the **no** form of this command to restore the default setting.

Syntax

[no] upgrade opcode auto

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ This command is used to enable or disable automatic upgrade of the operational code. When the switch starts up and automatic image upgrade is enabled by this command, the switch will follow these steps when it boots up:
 1. It will search for a new version of the image at the location specified by [upgrade opcode path](#) command. The name for the new image stored on the TFTP server must be ecs5610_52s.bix. If the switch detects a code version newer than the one currently in use, it will download the new image. If two code images are already stored in the switch, the image not set to start up the system will be overwritten by the new version.
 2. After the image has been downloaded, the switch will send a trap message to log whether or not the upgrade operation was successful.
 3. It sets the new version as the startup image.
 4. It then restarts the system to start using the new image.
- ◆ Any changes made to the default setting can be displayed with the [show running-config](#) or [show startup-config](#) commands.

Example

```
Console(config)#upgrade opcode auto
Console(config)#upgrade opcode path tftp://192.168.0.1/sm24/
Console(config)#
```

If a new image is found at the specified location, the following type of messages will be displayed during bootup.

```
:
Automatic Upgrade is looking for a new image
New image detected: current version 1.1.1.0; new version 1.1.1.2
Image upgrade in progress
The switch will restart after upgrade succeeds
Downloading new image
Flash programming started
Flash programming completed
The switch will now restart
:
```

upgrade opcode path This command specifies an TFTP server and directory in which the new opcode is stored. Use the **no** form of this command to clear the current setting.

Syntax

upgrade opcode path *opcode-dir-url*

no upgrade opcode path

opcode-dir-url - The location of the new code.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ This command is used in conjunction with the **upgrade opcode auto** command to facilitate automatic upgrade of new operational code stored at the location indicated by this command.
- ◆ The name for the new image stored on the TFTP server must be `ecs5610-52s.bix`. However, note that file name is not to be included in this command.
- ◆ When specifying a TFTP server, the following syntax must be used, where *filedir* indicates the path to the directory containing the new image:

```
tftp://192.168.0.1[/filedir]/
```
- ◆ When specifying an FTP server, the following syntax must be used, where *filedir* indicates the path to the directory containing the new image:

```
ftp://[username[:password@]]192.168.0.1[/filedir]/
```

If the user name is omitted, "anonymous" will be used for the connection. If the password is omitted a null string ("") will be used for the connection.

Example

This shows how to specify a TFTP server where new code is stored.

```
Console(config)#upgrade opcode path tftp://192.168.0.1/sm24/  
Console(config)#
```

This shows how to specify an FTP server where new code is stored.

```
Console(config)#upgrade opcode path ftp://admin:billy@192.168.0.1/sm24/  
Console(config)#
```

upgrade opcode reload This command reloads the switch automatically after the opcode upgrade is completed. Use the **no** form to disable this feature.

Syntax

[no] upgrade opcode reload

Default Setting

Disabled

Command Mode

Global Configuration

Example

This shows how to automatically reboot and load the new code after the opcode upgrade is completed.

```
Console(config)#upgrade opcode reload  
Console(config)#
```

show upgrade This command shows the opcode upgrade configuration settings.

Command Mode

Privileged Exec

Example

```
Console#show upgrade  
Auto Image Upgrade Global Settings:  
  Status      : Disabled  
  Reload Status : Disabled  
  Path        :  
  File Name   : ecs5610-52s.bix  
Console#
```

Line

You can access the onboard configuration program by attaching a VT100 compatible device to the server's serial port. These commands are used to set communication parameters for the serial port or Telnet (i.e., a virtual terminal).

Table 18: Line Commands

Command	Function	Mode
<code>line</code>	Identifies a specific line for configuration and starts the line configuration mode	GC
<code>accounting exec</code>	Applies an accounting method to local console, Telnet or SSH connections	LC
<code>authorization exec</code>	Applies an authorization method to local console, Telnet or SSH connections	LC
<code>databits*</code>	Sets the number of data bits per character that are interpreted and generated by hardware	LC
<code>exec-timeout</code>	Sets the interval that the command interpreter waits until user input is detected	LC
<code>login</code>	Enables password checking at login	LC
<code>parity*</code>	Defines the generation of a parity bit	LC
<code>password</code>	Specifies a password on a line	LC
<code>password-thresh</code>	Sets the password intrusion threshold, which limits the number of failed logon attempts	LC
<code>silent-time*</code>	Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the <code>password-thresh</code> command	LC
<code>speed*</code>	Sets the terminal baud rate	LC
<code>stopbits*</code>	Sets the number of the stop bits transmitted per byte	LC
<code>timeout login response</code>	Sets the interval that the system waits for a login attempt	LC
<code>disconnect</code>	Terminates a line connection	PE
<code>terminal</code>	Configures terminal settings, including escape-character, line length, terminal type, and width	PE
<code>show line</code>	Displays a terminal line's parameters	NE, PE

* These commands only apply to the serial port.

line This command identifies a specific line for configuration, and to process subsequent line configuration commands.

Syntax

line {**console** | **vty**}

console - Console terminal line.

vty - Virtual terminal for remote console access (i.e., Telnet).

Default Setting

There is no default line.

Command Mode

Global Configuration

Command Usage

Telnet is considered a virtual terminal connection and will be shown as “VTY” in screen displays such as [show users](#). However, the serial communication parameters (e.g., databits) do not affect Telnet connections.

Example

To enter console line mode, enter the following command:

```
Console(config)#line console
Console(config-line)#
```

Related Commands

[show line \(144\)](#)

[show users \(118\)](#)

databits This command sets the number of data bits per character that are interpreted and generated by the console port. Use the **no** form to restore the default value.

Syntax

databits {**7** | **8**}

no databits

7 - Seven data bits per character.

8 - Eight data bits per character.

Default Setting

8 data bits per character

Command Mode

Line Configuration

Command Usage

The **databits** command can be used to mask the high bit on input from devices that generate 7 data bits with parity. If parity is being generated, specify 7 data bits per character. If no parity is required, specify 8 data bits per character.

Example

To specify 7 data bits, enter this command:

```
Console(config-line)#databits 7
Console(config-line)#
```

Related Commands

[parity \(138\)](#)

exec-timeout This command sets the interval that the system waits until user input is detected. Use the **no** form to restore the default.

Syntax

exec-timeout [*seconds*]

no exec-timeout

seconds - Integer that specifies the timeout interval.
(Range: 60 - 65535 seconds; 0: no timeout)

Default Setting

600 seconds

Command Mode

Line Configuration

Command Usage

- ◆ If user input is detected within the timeout interval, the session is kept open; otherwise the session is terminated.
- ◆ This command applies to both the local console and Telnet connections.
- ◆ The timeout for Telnet cannot be disabled.
- ◆ Using the command without specifying a timeout restores the default setting.

Example

To set the timeout to two minutes, enter this command:

```
Console(config-line)#exec-timeout 120
Console(config-line)#
```


login This command enables password checking at login. Use the **no** form to disable password checking and allow connections without a password.

Syntax

login [local]

no login

local - Selects local password checking. Authentication is based on the user name specified with the [username](#) command.

Default Setting

login local

Command Mode

Line Configuration

Command Usage

- ◆ There are three authentication modes provided by the switch itself at login:
 - **login** selects authentication by a single global password as specified by the [password](#) line configuration command. When using this method, the management interface starts in Normal Exec (NE) mode.
 - **login local** selects authentication via the user name and password specified by the [username](#) command (i.e., default setting). When using this method, the management interface starts in Normal Exec (NE) or Privileged Exec (PE) mode, depending on the user's privilege level (0 or 15 respectively).
 - **no login** selects no authentication. When using this method, the management interface starts in Normal Exec (NE) mode.
- ◆ This command controls login authentication via the switch itself. To configure user names and passwords for remote authentication servers, you must use the RADIUS or TACACS software installed on those servers.

Example

```
Console(config-line)#login local
Console(config-line)#
```

Related Commands

[username \(219\)](#)

[password \(138\)](#)

parity This command defines the generation of a parity bit. Use the **no** form to restore the default setting.

Syntax

parity {**none** | **even** | **odd**}

no parity

none - No parity

even - Even parity

odd - Odd parity

Default Setting

No parity

Command Mode

Line Configuration

Command Usage

Communication protocols provided by devices such as terminals and modems often require a specific parity bit setting.

Example

To specify no parity, enter this command:

```
Console(config-line)#parity none
Console(config-line)#
```

password This command specifies the password for a line. Use the **no** form to remove the password.

Syntax

password {**0** | **7**} *password*

no password

{**0** | **7**} - 0 means plain password, 7 means encrypted password

password - Character string that specifies the line password.

(Maximum length: 32 characters plain text or encrypted, case sensitive)

Default Setting

No password is specified.

Command Mode

Line Configuration

Command Usage

- ◆ When a connection is started on a line with password protection, the system prompts for the password. If you enter the correct password, the system shows a prompt. You can use the [password-thresh](#) command to set the number of times a user can enter an incorrect password before the system terminates the line connection and returns the terminal to the idle state.
- ◆ The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

```
Console(config-line)#password 0 secret
Console(config-line)#
```

Related Commands

[login \(137\)](#)

[password-thresh \(139\)](#)

password-thresh This command sets the password intrusion threshold which limits the number of failed logon attempts. Use the **no** form to remove the threshold value.

Syntax

password-thresh [*threshold*]

no password-thresh

threshold - The number of allowed password attempts. (Range: 1-120; 0: no threshold)

Default Setting

The default value is three attempts.

Command Mode

Line Configuration

Command Usage

When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time before allowing the next logon attempt. (Use the [silent-time](#) command to set this interval.) When this threshold is reached for Telnet, the Telnet logon interface shuts down.

Example

To set the password threshold to five attempts, enter this command:

```
Console(config-line)#password-thresh 5
Console(config-line)#
```

Related Commands

[silent-time \(140\)](#)

silent-time This command sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the [password-thresh](#) command. Use the **no** form to remove the silent time value.

Syntax

silent-time [*seconds*]

no silent-time

seconds - The number of seconds to disable console response.
(Range: 1-65535; where 0 means disabled)

Default Setting

Disabled

Command Mode

Line Configuration

Example

To set the silent time to 60 seconds, enter this command:

```
Console(config-line)#silent-time 60
Console(config-line)#
```

Related Commands

[password-thresh \(139\)](#)

speed This command sets the terminal line's baud rate. This command sets both the transmit (to terminal) and receive (from terminal) speeds. Use the **no** form to restore the default setting.

Syntax

speed *bps*

no speed

bps - Baud rate in bits per second.

(Options: 9600, 19200, 38400, 57600, 115200 bps)

Default Setting

115200 bps

Command Mode

Line Configuration

Command Usage

Set the speed to match the baud rate of the device connected to the serial port. Some baud rates available on devices connected to the port might not be supported. The system indicates if the speed you selected is not supported.

Example

To specify 57600 bps, enter this command:

```
Console(config-line)#speed 57600
Console(config-line)#
```

stopbits This command sets the number of the stop bits transmitted per byte. Use the **no** form to restore the default setting.

Syntax

stopbits {**1** | **2**}

no stopbits

1 - One stop bit

2 - Two stop bits

Default Setting

1 stop bit

Command Mode

Line Configuration

Example

To specify 2 stop bits, enter this command:

```
Console(config-line)#stopbits 2
Console(config-line)#
```

timeout login response This command sets the interval that the system waits for a user to log into the CLI. Use the **no** form to restore the default setting.

Syntax

timeout login response [*seconds*]

no timeout login response

seconds - Integer that specifies the timeout interval.
(Range: 10 - 300 seconds)

Default Setting

300 seconds

Command Mode

Line Configuration

Command Usage

- ◆ If a login attempt is not detected within the timeout interval, the connection is terminated for the session.
- ◆ This command applies to both the local console and Telnet connections.
- ◆ The timeout for Telnet cannot be disabled.
- ◆ Using the command without specifying a timeout restores the default setting.

Example

To set the timeout to two minutes, enter this command:

```
Console(config-line)#timeout login response 120
Console(config-line)#
```

disconnect This command terminates an SSH, Telnet, or console connection.

Syntax

disconnect *session-id*

session-id – The session identifier for an SSH, Telnet or console connection.
(Range: 0-8)

Command Mode

Privileged Exec

Command Usage

Specifying session identifier “0” will disconnect the console connection. Specifying any other identifiers for an active session will disconnect an SSH or Telnet connection.

Example

```
Console#disconnect 1
Console#
```

Related Commands

[show ssh \(252\)](#)

[show users \(118\)](#)

terminal This command configures terminal settings, including escape-character, lines displayed, terminal type, width, and command history. Use the **no** form with the appropriate keyword to restore the default setting.

Syntax

terminal {**escape-character** {**ASCII-number** | *character*} | **history** [**size** *size*] | **length** *length* | **terminal-type** {**ansi-bbs** | **vt-100** | **vt-102**} | **width** *width*}

escape-character - The keyboard character used to escape from current line input.

ASCII-number - ASCII decimal equivalent. (Range: 0-255)

character - Any valid keyboard character.

history - The number of lines stored in the command buffer, and recalled using the arrow keys. (Range: 0-256)

length - The number of lines displayed on the screen. (Range: 0-512, where 0 means not to pause)

terminal-type - The type of terminal emulation used.

ansi-bbs - ANSI-BBS

vt-100 - VT-100

vt-102 - VT-102

width - The number of character columns displayed on the terminal.
(Range: 0-80)

Default Setting

Escape Character: 27 (ASCII-number)

History: 10

Length: 24

Terminal Type: VT100

Width: 80

Command Mode

Privileged Exec

Example

This example sets the number of lines displayed by commands with lengthy output such as [show running-config](#) to 48 lines.

```
Console#terminal length 48
Console#
```

show line This command displays the terminal line's parameters.

Syntax

show line [**console** | **vty**]

console - Console terminal line.

vty - Virtual terminal for remote console access (i.e., Telnet).

Default Setting

Shows all lines

Command Mode

Normal Exec, Privileged Exec

Example

To show all lines, enter this command:

```
Console#show line
Console Configuration:
  Password Threshold : 3 times
  EXEC Timeout       : 600 seconds
  Login Timeout      : 300 seconds
  Silent Time        : Disabled
  Baud Rate          : 115200
  Data Bits          : 8
  Parity             : None
  Stop Bits          : 1
```



```

VTY Configuration:
  Password Threshold : 3 times
  Inactive Timeout   : 600 seconds
  Login Timeout      : 300 sec.
  Silent Time        : Disabled
Console#

```

Event Logging

This section describes commands used to configure event logging on the switch.

Table 19: Event Logging Commands

Command	Function	Mode
logging facility	Sets the facility type for remote logging of syslog messages	GC
logging history	Limits syslog messages saved to switch memory based on severity	GC
logging host	Adds a syslog server host IP address that will receive logging messages	GC
logging on	Controls logging of error messages	GC
logging trap	Limits syslog messages saved to a remote server based on severity	GC
clear log	Clears messages from the logging buffer	PE
show log	Displays log messages	PE
show logging	Displays the state of logging	PE

logging facility This command sets the facility type for remote logging of syslog messages. Use the **no** form to return the type to the default.

Syntax

logging facility *type*

no logging facility

type - A number that indicates the facility used by the syslog server to dispatch log messages to an appropriate service. (Range: 16-23)

Default Setting

23

Command Mode

Global Configuration

Command Usage

The command specifies the facility type tag sent in syslog messages. (See RFC 3164.) This type has no effect on the kind of messages reported by the switch.

However, it may be used by the syslog server to sort messages or to store messages in the corresponding database.

Example

```
Console(config)#logging facility 19
Console(config)#
```

logging history This command limits syslog messages saved to switch memory based on severity. The **no** form returns the logging of syslog messages to the default level.

Syntax

logging history {flash | ram} level

no logging history {flash | ram}

flash - Event history stored in flash memory (i.e., permanent memory).

ram - Event history stored in temporary RAM (i.e., memory flushed on power reset).

level - One of the levels listed below. Messages sent include the selected level down to level 0. (Range: 0-7)

Table 20: Logging Levels

Level	Severity Name	Description
7	debugging	Debugging messages
6	informational	Informational messages only
5	notifications	Normal but significant condition, such as cold start
4	warnings	Warning conditions (e.g., return false, unexpected return)
3	errors	Error conditions (e.g., invalid input, default used)
2	critical	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
1	alerts	Immediate action needed
0	emergencies	System unusable

Default Setting

Flash: errors (level 3 - 0)

RAM: debugging (level 7 - 0)

Command Mode

Global Configuration

Command Usage

The message level specified for flash memory must be a higher priority (i.e., numerically lower) than that specified for RAM.

Example

```
Console(config)#logging history ram 0  
Console(config)#
```

logging host This command adds a syslog server host IP address that will receive logging messages. Use the **no** form to remove a syslog server host.

Syntax

[no] logging host *host-ip-address* [**port** *udp-port*]

host-ip-address - The IPv4 or IPv6 address of a syslog server.

udp-port - The UDP port number used by the remote server.
(Range: 1-65535)

Default Setting

Host: None

UPD Port: 514

Command Mode

Global Configuration

Command Usage

- ◆ Use this command more than once to build up a list of host IP addresses.
- ◆ The maximum number of host IP addresses allowed is five.

Example

```
Console(config)#logging host 10.1.0.3  
Console(config)#
```

logging on This command controls logging of error messages, sending debug or error messages to a logging process. The **no** form disables the logging process.

Syntax

[no] logging on

Default Setting

None

Command Mode

Global Configuration

Command Usage

The logging process controls error messages saved to switch memory or sent to remote syslog servers. You can use the [logging history](#) command to control the type of error messages that are stored in memory. You can use the [logging trap](#) command to control the type of error messages that are sent to specified syslog servers.

Example

```
Console(config)#logging on
Console(config)#
```

Related Commands

[logging history \(146\)](#)

[logging trap \(148\)](#)

[clear log \(149\)](#)

logging trap This command enables the logging of system messages to a remote server, or limits the syslog messages saved to a remote server based on severity. Use this command without a specified level to enable remote logging. Use the **no** form to disable remote logging.

Syntax

logging trap [level *level*]

no logging trap [level]

level - One of the syslog severity levels listed in the table on [page 146](#).
Messages sent include the selected level through level 0.

Default Setting

Disabled

Level 7

Command Mode

Global Configuration

Command Usage

- ◆ Using this command with a specified level enables remote logging and sets the minimum severity level to be saved.
- ◆ Using this command without a specified level also enables remote logging, but restores the minimum severity level to the default.

Example

```
Console(config)#logging trap 4
Console(config)#
```

clear log This command clears messages from the log buffer.

Syntax

clear log [**flash** | **ram**]

flash - Event history stored in flash memory (i.e., permanent memory).

ram - Event history stored in temporary RAM (i.e., memory flushed on power reset).

Default Setting

Flash and RAM

Command Mode

Privileged Exec

Example

```
Console#clear log
Console#
```

Related Commands

[show log \(149\)](#)

show log This command displays the log messages stored in local memory.

Syntax

show log {**flash** | **ram**}

flash - Event history stored in flash memory (i.e., permanent memory).

ram - Event history stored in temporary RAM (i.e., memory flushed on power reset).

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- ◆ All log messages are retained in RAM and Flash after a warm restart (i.e., power is reset through the command interface).
- ◆ All log messages are retained in Flash and purged from RAM after a cold restart (i.e., power is turned off and then on through the power source).

Example

The following example shows the event message stored in RAM.

```
Console#show log ram
[1] 00:01:30 2001-01-01
    "VLAN 1 link-up notification."
    level: 6, module: 5, function: 1, and event no.: 1
[0] 00:01:30 2001-01-01
    "Unit 1, Port 1 link-up notification."
    level: 6, module: 5, function: 1, and event no.: 1
Console#
```

show logging This command displays the configuration settings for logging messages to local switch memory, to an SMTP event handler, or to a remote syslog server.

Syntax

show logging {flash | ram | sendmail | trap}

flash - Displays settings for storing event messages in flash memory (i.e., permanent memory).

ram - Displays settings for storing event messages in temporary RAM (i.e., memory flushed on power reset).

sendmail - Displays settings for the SMTP event handler ([page 155](#)).

trap - Displays settings for the trap function.

Default Setting

None

Command Mode

Privileged Exec

Example

The following example shows that system logging is enabled, the message level for flash memory is "errors" (i.e., default level 3 - 0), and the message level for RAM is "debugging" (i.e., default level 7 - 0).

```
Console#show logging flash
Syslog logging:      Enabled
History logging in FLASH: level errors
Console#show logging ram
Syslog logging:      Enabled
History logging in RAM: level debugging
Console#
```

Table 21: show logging flash/ram - display description

Field	Description
Syslog logging	Shows if system logging has been enabled via the logging on command.
History logging in FLASH	The message level(s) reported based on the logging history command.
History logging in RAM	The message level(s) reported based on the logging history command.

The following example displays settings for the trap function.

```

Console#show logging trap
Remote Log Status           : Disabled
Remote Log Facility Type    : Local use 7
Remote Log Level Type       : Debugging messages
Remote Log Server IP Address : 0.0.0.0
Remote Log Server IP Address : 0.0.0.0
Remote Log Server IP Address : 0.0.0.0
Remote Log Server IP Address : 0.0.0.0
Remote Log Server IP Address : 0.0.0.0
Console#

```

Table 22: show logging trap - display description

Field	Description
Syslog logging	Shows if system logging has been enabled via the logging on command.
REMOTELOG status	Shows if remote logging has been enabled via the logging trap command.
REMOTELOG facility type	The facility type for remote logging of syslog messages as specified in the logging facility command.
REMOTELOG level type	The severity threshold for syslog messages sent to a remote server as specified in the logging trap command.
REMOTELOG server IP address	The address of syslog servers as specified in the logging host command.

Related Commands

[show logging sendmail \(155\)](#)

SMTP Alerts

These commands configure SMTP event handling, and forwarding of alert messages to the specified SMTP servers and email recipients.

Table 23: Event Logging Commands

Command	Function	Mode
<code>logging sendmail</code>	Enables SMTP event handling	GC
<code>logging sendmail host</code>	SMTP servers to receive alert messages	GC
<code>logging sendmail level</code>	Severity threshold used to trigger alert messages	GC
<code>logging sendmail destination-email</code>	Email recipients of alert messages	GC
<code>logging sendmail source-email</code>	Email address used for “From” field of alert messages	GC
<code>show logging sendmail</code>	Displays SMTP event handler settings	NE, PE

logging sendmail This command enables SMTP event handling. Use the **no** form to disable this function.

Syntax

[no] logging sendmail

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#logging sendmail
Console(config)#
```

logging sendmail host This command specifies SMTP servers that will be sent alert messages. Use the **no** form to remove an SMTP server.

Syntax

[no] logging sendmail host *ip-address*

ip-address - IPv4 or IPv6 address of an SMTP server that will be sent alert messages for event handling.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ You can specify up to three SMTP servers for event handling. However, you must enter a separate command to specify each server.
- ◆ To send email alerts, the switch first opens a connection, sends all the email alerts waiting in the queue one by one, and finally closes the connection.
- ◆ To open a connection, the switch first selects the server that successfully sent mail during the last connection, or the first server configured by this command. If it fails to send mail, the switch selects the next server in the list and tries to send mail again. If it still fails, the system will repeat the process at a periodic interval. (A trap will be triggered if the switch cannot successfully open a connection.)

Example

```
Console(config)#logging sendmail host 192.168.1.19  
Console(config)#
```

logging sendmail level This command sets the severity threshold used to trigger alert messages. Use the **no** form to restore the default setting.

Syntax

logging sendmail level *level*

no logging sendmail level

level - One of the system message levels ([page 146](#)). Messages sent include the selected level down to level 0. (Range: 0-7; Default: 7)

Default Setting

Level 7

Command Mode

Global Configuration

Command Usage

The specified level indicates an event threshold. All events at this level or higher will be sent to the configured email recipients. (For example, using Level 7 will report all events from level 7 to level 0.)

Example

This example will send email alerts for system errors from level 3 through 0.

```
Console(config)#logging sendmail level 3  
Console(config)#
```

logging sendmail destination-email

This command specifies the email recipients of alert messages. Use the **no** form to remove a recipient.

Syntax

[no] logging sendmail destination-email *email-address*

email-address - The source email address used in alert messages.
(Range: 1-41 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

You can specify up to five recipients for alert messages. However, you must enter a separate command to specify each recipient.

Example

```
Console(config)#logging sendmail destination-email ted@this-company.com  
Console(config)#
```

logging sendmail source-email

This command sets the email address used for the “From” field in alert messages. Use the **no** form to restore the default value.

Syntax

logging sendmail source-email *email-address*

no logging sendmail source-email

email-address - The source email address used in alert messages.
(Range: 1-41 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

You may use an symbolic email address that identifies the switch, or the address of an administrator responsible for the switch.

Example

```
Console(config)#logging sendmail source-email bill@this-company.com
Console(config)#
```

**show logging
sendmail** This command displays the settings for the SMTP event handler.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show logging sendmail
SMTP servers
-----
192.168.1.19

SMTP Minimum Severity Level: 7

SMTP Destination E-mail Addresses
-----
ted@this-company.com

SMTP Source Email Address: bill@this-company.com

SMTP Status: Enabled
Console#
```

Time

The system clock can be dynamically set by polling a set of specified time servers (NTP or SNTP). Maintaining an accurate time on the switch enables the system log to record meaningful dates and times for event entries. If the clock is not set, the switch will only record the time from the factory default set at the last bootup.

Table 24: Time Commands

Command	Function	Mode
<i>SNTP Commands</i>		
sntp client	Accepts time from specified time servers	GC
sntp poll	Sets the interval at which the client polls for time	GC
sntp server	Specifies one or more time servers	GC
show sntp	Shows current SNTP configuration settings	NE, PE

Table 24: Time Commands (Continued)

Command	Function	Mode
<i>NTP Commands</i>		
<code>ntp authenticate</code>	Enables authentication for NTP traffic	GC
<code>ntp authentication-key</code>	Configures authentication keys	GC
<code>ntp client</code>	Enables the NTP client for time updates from specified servers	GC
<code>ntp server</code>	Specifies NTP servers to poll for time updates	GC
<code>show ntp</code>	Shows current NTP configuration settings	NE, PE
<i>Manual Configuration Commands</i>		
<code>clock summer-time (date)</code>	Configures summer time* for the switch's internal clock	GC
<code>clock summer-time (predefined)</code>	Configures summer time for the switch's internal clock	GC
<code>clock summer-time (recurring)</code>	Configures summer time for the switch's internal clock	GC
<code>clock timezone</code>	Sets the time zone for the switch's internal clock	GC
<code>calendar set</code>	Sets the system date and time	PE
<code>show calendar</code>	Displays the current date and time setting	NE, PE

* Daylight savings time.

SNTP Commands

sntp client This command enables SNTP client requests for time synchronization from NTP or SNTP time servers specified with the `sntp server` command. Use the **no** form to disable SNTP client requests.

Syntax

[no] sntp client

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ The time acquired from time servers is used to record accurate dates and times for log events. Without SNTP, the switch only records the time starting from the factory default set at the last bootstrap (i.e., 00:00:00, Jan. 1, 2001).
- ◆ This command enables client time requests to time servers specified via the `sntp server` command. It issues time synchronization requests based on the interval set via the `sntp poll` command.

Example

```
Console(config)#ntp server 10.1.0.19
Console(config)#ntp poll 60
Console(config)#ntp client
Console(config)#end
Console#show ntp
Current Time   : Mar 12 02:33:00 2013
Poll Interval  : 60 seconds
Current Mode    : Unicast
SNTP Status     : Enabled
SNTP Server     : 10.1.0.19
Current Server  : 137.92.140.80
Console#
```

Related Commands

[ntp server \(158\)](#)

[ntp poll \(157\)](#)

[show ntp \(158\)](#)

ntp poll This command sets the interval between sending time requests when the switch is set to SNTP client mode. Use the **no** form to restore to the default.

Syntax

ntp poll *seconds*

no ntp poll

seconds - Interval between time requests. (Range: 16-16384 seconds)

Default Setting

16 seconds

Command Mode

Global Configuration

Example

```
Console(config)#ntp poll 60
Console#
```

Related Commands

[ntp client \(156\)](#)

sntp server This command sets the IP address of the servers to which SNTP time requests are issued. Use the this command with no arguments to clear all time servers from the current list. Use the **no** form to clear all time servers from the current list, or to clear a specific server.

Syntax

sntp server [*ip1* [*ip2* [*ip3*]]]

no sntp server [*ip1* [*ip2* [*ip3*]]]

ip - IPv4/v6 address of a time server (NTP or SNTP). (Range: 1 - 3 addresses)

Default Setting

None

Command Mode

Global Configuration

Command Usage

This command specifies time servers from which the switch will poll for time updates when set to SNTP client mode. The client will poll the time servers in the order specified until a response is received. It issues time synchronization requests based on the interval set via the [sntp poll](#) command.

Example

```
Console(config)#sntp server 10.1.0.19
Console#
```

Related Commands

[sntp client \(156\)](#)

[sntp poll \(157\)](#)

[show sntp \(158\)](#)

show sntp This command displays the current time and configuration settings for the SNTP client, and indicates whether or not the local time has been properly updated.

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command displays the current time, the poll interval used for sending time synchronization requests, and the current SNTP mode (i.e., unicast).

Example

```
Console#show sntp
Current Time   : Nov  5 18:51:22 2006
Poll Interval  : 16 seconds
Current Mode   : Unicast
SNTP Status    : Enabled
SNTP Server    : 137.92.140.80
Current Server : 137.92.140.80
Console#
```

NTP Commands

ntp authenticate This command enables authentication for NTP client-server communications. Use the **no** form to disable authentication.

Syntax

[no] ntp authenticate

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

You can enable NTP authentication to ensure that reliable updates are received from only authorized NTP servers. The authentication keys and their associated key number must be centrally managed and manually distributed to NTP servers and clients. The key numbers and key values must match on both the server and client.

Example

```
Console(config)#ntp authenticate
Console(config)#
```

Related Commands

[ntp authentication-key \(160\)](#)

ntp authentication-key This command configures authentication keys and key numbers to use when NTP authentication is enabled. Use the **no** form of the command to clear a specific authentication key or all keys from the current list.

Syntax

ntp authentication-key *number* **md5** *key*

no ntp authentication-key [*number*]

number - The NTP authentication key ID number. (Range: 1-65535)

md5 - Specifies that authentication is provided by using the message digest algorithm 5.

key - An MD5 authentication key string. The key string can be up to 32 case-sensitive printable ASCII characters (no spaces).

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ The key number specifies a key value in the NTP authentication key list. Up to 255 keys can be configured on the switch. Re-enter this command for each server you want to configure.
- ◆ Note that NTP authentication key numbers and values must match on both the server and client.
- ◆ NTP authentication is optional. When enabled with the **ntp authenticate** command, you must also configure at least one key number using this command.
- ◆ Use the **no** form of this command without an argument to clear all authentication keys in the list.

Example

```
Console(config)#ntp authentication-key 45 md5 thisiskey45
Console(config)#
```

Related Commands

[ntp authenticate \(159\)](#)

ntp client This command enables NTP client requests for time synchronization from NTP time servers specified with the **ntp servers** command. Use the **no** form to disable NTP client requests.

Syntax

[no] ntp client

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ The SNTP and NTP clients cannot be enabled at the same time. First disable the SNTP client before using this command.
- ◆ The time acquired from time servers is used to record accurate dates and times for log events. Without NTP, the switch only records the time starting from the factory default set at the last bootup (i.e., 00:00:00, Jan. 1, 2001).
- ◆ This command enables client time requests to time servers specified via the **ntp servers** command. It issues time synchronization requests based on the interval set via the **ntp poll** command.

Example

```
Console(config)#ntp client
Console(config)#
```

Related Commands

[sntp client \(156\)](#)

[ntp server \(161\)](#)

ntp server This command sets the IP addresses of the servers to which NTP time requests are issued. Use the **no** form of the command to clear a specific time server or all servers from the current list.

Syntax

ntp server *ip-address* [**key** *key-number*]

no ntp server [*ip-address*]

ip-address - IP address of an NTP time server.

key-number - The number of an authentication key to use in communications with the server. (Range: 1-65535)

Default Setting

Version number: 3

Command Mode

Global Configuration

Command Usage

- ◆ This command specifies time servers that the switch will poll for time updates when set to NTP client mode. It issues time synchronization requests based on the interval set with the **ntp poll** command. The client will poll all the time servers configured, the responses received are filtered and compared to determine the most reliable and accurate time update for the switch.
- ◆ You can configure up to 50 NTP servers on the switch. Re-enter this command for each server you want to configure.
- ◆ NTP authentication is optional. If enabled with the **ntp authenticate** command, you must also configure at least one key number using the **ntp authentication-key** command.
- ◆ Use the **no** form of this command without an argument to clear all configured servers in the list.

Example

```
Console(config)#ntp server 192.168.3.20
Console(config)#ntp server 192.168.3.21
Console(config)#ntp server 192.168.5.23 key 19
Console(config)#
```

Related Commands

[ntp client \(161\)](#)

[show ntp \(162\)](#)

show ntp This command displays the current time and configuration settings for the NTP client, and indicates whether or not the local time has been properly updated.

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command displays the current time, the poll interval used for sending time synchronization requests, and the current NTP mode (i.e., unicast).

Example

```
Console#show ntp
Current Time           : Apr 29 13:57:32 2011
Polling                : 1024 seconds
Current Mode           : unicast
```

```

NTP Status           : Enabled
NTP Authenticate Status : Enabled
Last Update NTP Server : 192.168.0.88      Port: 123
Last Update Time      : Mar 12 02:41:01 2013 UTC
NTP Server 192.168.0.88 version 3
NTP Server 192.168.3.21 version 3
NTP Server 192.168.4.22 version 3 key 19
NTP Authentication Key 19 md5 42V68751663T6K11P2J307210R885
Console#

```

Manual Configuration Commands

clock summer-time (date) This command sets the start, end, and offset times of summer time (daylight savings time) for the switch on a one-time basis. Use the **no** form to disable summer time.

Syntax

clock summer-time *name* **date** *b-date b-month b-year b-hour b-minute e-date e-month e-year e-hour e-minute [offset]*

no clock summer-time

name - Name of the time zone while summer time is in effect, usually an acronym. (Range: 1-30 characters)

b-date - Day of the month when summer time will begin. (Range: 1-31)

b-month - The month when summer time will begin. (Options: **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december**)

b-year - The year summer time will begin.

b-hour - The hour summer time will begin. (Range: 0-23 hours)

b-minute - The minute summer time will begin. (Range: 0-59 minutes)

e-date - Day of the month when summer time will end. (Range: 1-31)

e-month - The month when summer time will end. (Options: **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december**)

e-year - The year summer time will end.

e-hour - The hour summer time will end. (Range: 0-23 hours)

e-minute - The minute summer time will end. (Range: 0-59 minutes)

offset - Summer time offset from the regular time zone, in minutes. (Range: 0-99 minutes)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ In some countries or regions, clocks are adjusted through the summer months so that afternoons have more daylight and mornings have less. This is known as Summer Time, or Daylight Savings Time (DST). Typically, clocks are adjusted forward one hour at the start of spring and then adjusted backward in autumn.
- ◆ This command sets the summer-time zone relative to the currently configured time zone. To specify a time corresponding to your local time when summer time is in effect, you must indicate the number of minutes your summer-time zone deviates from your regular time zone.

Example

```
Console(config)#clock summer-time DEST date april 1 2007 23 23 april 23 2007
23 23 60
Console(config)#
```

Related Commands

[show sntp \(158\)](#)

clock summer-time (predefined) This command configures the summer time (daylight savings time) status and settings for the switch using predefined configurations for several major regions in the world. Use the **no** form to disable summer time.

Syntax

clock summer-time *name* **predefined** [**australia** | **europe** | **new-zealand** | **usa**]

no clock summer-time

name - Name of the timezone while summer time is in effect, usually an acronym. (Range: 1-30 characters)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ In some countries or regions, clocks are adjusted through the summer months so that afternoons have more daylight and mornings have less. This is known as Summer Time, or Daylight Savings Time (DST). Typically, clocks are adjusted forward one hour at the start of spring and then adjusted backward in autumn.

- ◆ This command sets the summer-time relative to the configured time zone. To specify the time corresponding to your local time when summer time is in effect, select the predefined summer-time zone appropriate for your location, or manually configure summer time if these predefined configurations do not apply to your location (see [clock summer-time \(date\)](#) or [clock summer-time \(recurring\)](#)).

Table 25: Predefined Summer-Time Parameters

Region	Start Time, Day, Week, & Month	End Time, Day, Week, & Month	Rel. Offset
Australia	00:00:00, Sunday, Week 5 of October	23:59:59, Sunday, Week 5 of March	60 min
Europe	00:00:00, Sunday, Week 5 of March	23:59:59, Sunday, Week 5 of October	60 min
New Zealand	00:00:00, Sunday, Week 1 of October	23:59:59, Sunday, Week 3 of March	60 min
USA	00:00:00, Sunday, Week 2 of March	23:59:59, Sunday, Week 1 of November	60 min

Example

```
Console(config)#clock summer-time MESZ predefined europe
Console(config)#
```

Related Commands

[show sntp \(158\)](#)

clock summer-time (recurring) This command allows the user to manually configure the start, end, and offset times of summer time (daylight savings time) for the switch on a recurring basis. Use the **no** form to disable summer-time.

Syntax

clock summer-time *name* **recurring** *b-week b-day b-month b-hour b-minute e-week e-day e-month e-hour e-minute [offset]*

no clock summer-time

name - Name of the timezone while summer time is in effect, usually an acronym. (Range: 1-30 characters)

b-week - The week of the month when summer time will begin. (Range: 1-5)

b-day - The day of the week when summer time will begin. (Options: **sunday** | **monday** | **tuesday** | **wednesday** | **thursday** | **friday** | **saturday**)

b-month - The month when summer time will begin. (Options: **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december**)

b-hour - The hour when summer time will begin. (Range: 0-23 hours)

b-minute - The minute when summer time will begin. (Range: 0-59 minutes)

e-week - The week of the month when summer time will end. (Range: 1-5)

e-day - The day of the week summer time will end. (Options: **sunday** | **monday** | **tuesday** | **wednesday** | **thursday** | **friday** | **saturday**)

e-month - The month when summer time will end. (Options: **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december**)

e-hour - The hour when summer time will end. (Range: 0-23 hours)

e-minute - The minute when summer time will end. (Range: 0-59 minutes)

offset - Summer-time offset from the regular time zone, in minutes. (Range: 0-99 minutes)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ In some countries or regions, clocks are adjusted through the summer months so that afternoons have more daylight and mornings have less. This is known as Summer Time, or Daylight Savings Time (DST). Typically, clocks are adjusted forward one hour at the start of spring and then adjusted backward in autumn.
- ◆ This command sets the summer-time zone relative to the currently configured time zone. To display a time corresponding to your local time when summer time is in effect, you must indicate the number of minutes your summer-time zone deviates from your regular time zone.

Example

```
Console(config)#clock summer-time MESZ recurring 1 friday june 23 59 3
saturday september 2 55 60
Console(config)#
```

Related Commands

[show sntp \(158\)](#)

clock timezone This command sets the time zone for the switch's internal clock.

Syntax

clock timezone *name* **hour** *hours* **minute** *minutes*
{**before-utc** | **after-utc**}

name - Name of timezone, usually an acronym. (Range: 1-30 characters)

hours - Number of hours before/after UTC. (Range: 0-12 hours before UTC, 0-13 hours after UTC)

minutes - Number of minutes before/after UTC. (Range: 0-59 minutes)

before-utc - Sets the local time zone before (east) of UTC.

after-utc - Sets the local time zone after (west) of UTC.

Default Setting

None

Command Mode

Global Configuration

Command Usage

This command sets the local time zone relative to the Coordinated Universal Time (UTC, formerly Greenwich Mean Time or GMT), based on the earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (before) or west (after) of UTC.

Example

```
Console(config)#clock timezone Japan hours 8 minute 0 after-UTC
Console(config)#
```

Related Commands

[show sntp \(158\)](#)

calendar set This command sets the system clock. It may be used if there is no time server on your network, or if you have not configured the switch to receive signals from a time server.

Syntax

calendar set *hour min sec* {*day month year* | *month day year*}

hour - Hour in 24-hour format. (Range: 0 - 23)

min - Minute. (Range: 0 - 59)

sec - Second. (Range: 0 - 59)

day - Day of month. (Range: 1 - 31)

month - **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december**

year - Year (4-digit). (Range: 1970-2037)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Note that when SNTP is enabled, the system clock cannot be manually configured.

Example

This example shows how to set the system clock to 15:12:34, February 1st, 2011.

```
Console#calendar set 15 12 34 1 February 2011
Console#
```

show calendar This command displays the system clock.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show calendar
Current Time      : Mar 12 02:53:58 2013
Time Zone        : UTC, 00:00
Summer Time      : DEST, offset 60 minutes
                  Apr 1 2007 23:23 to Apr 23 2007 23:23
Summer Time in Effect : No
Console#
```


Time Range

This section describes the commands used to sets a time range for use by other functions, such as Access Control Lists.

Table 26: Time Range Commands

Command	Function	Mode
time-range	Specifies the name of a time range, and enters time range configuration mode	GC
absolute	Sets the time range for the execution of a command	TR
periodic	Sets the time range for the periodic execution of a command	TR
show time-range	Shows configured time ranges.	PE

time-range This command specifies the name of a time range, and enters time range configuration mode. Use the **no** form to remove a previously specified time range.

Syntax

[no] time-range *name*

name - Name of the time range. (Range: 1-16 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

This command sets a time range for use by other functions, such as Access Control Lists.

Example

```
Console(config)#time-range r&d
Console(config-time-range)#
```

Related Commands

[Access Control Lists \(347\)](#)

absolute This command sets the time range for the execution of a command. Use the **no** form to remove a previously specified time.

Syntax

absolute start *hour minute day month year*
[**end** *hour minutes day month year*]

absolute end *hour minutes day month year*

no absolute

hour - Hour in 24-hour format. (Range: 0-23)

minute - Minute. (Range: 0-59)

day - Day of month. (Range: 1-31)

month - **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** |
september | **october** | **november** | **december**

year - Year (4-digit). (Range: 2009-2109)

Default Setting

None

Command Mode

Time Range Configuration

Command Usage

- ◆ If a time range is already configured, you must use the **no** form of this command to remove the current entry prior to configuring a new time range.
- ◆ If both an absolute rule and one or more periodic rules are configured for the same time range (i.e., named entry), that entry will only take effect if the current time is within the absolute time range and one of the periodic time ranges.

Example

This example configures the time for the single occurrence of an event.

```
Console(config)#time-range r&d
Console(config-time-range)#absolute start 1 1 1 april 2009 end 2 1 1 april
2009
Console(config-time-range)#
```

periodic This command sets the time range for the periodic execution of a command. Use the **no** form to remove a previously specified time range.

Syntax

[no] periodic {daily | friday | monday | saturday | sunday | thursday | tuesday | wednesday | weekdays | weekend} hour minute to {daily | friday | monday | saturday | sunday | thursday | tuesday | wednesday | weekdays | weekend} hour minute}

daily - Daily

friday - Friday

monday - Monday

saturday - Saturday

sunday - Sunday

thursday - Thursday

tuesday - Tuesday

wednesday - Wednesday

weekdays - Weekdays

weekend - Weekends

hour - Hour in 24-hour format. (Range: 0-23)

minute - Minute. (Range: 0-59)

Default Setting

None

Command Mode

Time Range Configuration

Command Usage

- ◆ If a time range is already configured, you must use the **no** form of this command to remove the current entry prior to configuring a new time range.
- ◆ If both an absolute rule and one or more periodic rules are configured for the same time range (i.e., named entry), that entry will only take effect if the current time is within the absolute time range and one of the periodic time ranges.

Example

This example configures a time range for the periodic occurrence of an event.

```
Console(config)#time-range sales
Console(config-time-range)#periodic daily 1 1 to 2 1
Console(config-time-range)#
```

show time-range This command shows configured time ranges.

Syntax

show time-range *[name]*

name - Name of the time range. (Range: 1-30 characters)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show time-range r&d
Time-range r&d:
  absolute start 01:01 01 April 2009
  periodic      Daily 01:01 to      Daily 02:01
  periodic      Daily 02:01 to      Daily 03:01
Console#
```

Switch Clustering

Switch Clustering is a method of grouping switches together to enable centralized management through a single unit. Switches that support clustering can be grouped together regardless of physical location or switch type, as long as they are connected to the same local network.

Table 27: Switch Cluster Commands

Command	Function	Mode
cluster	Configures clustering on the switch	GC
cluster commander	Configures the switch as a cluster Commander	GC
cluster ip-pool	Sets the cluster IP address pool for Members	GC
cluster member	Sets Candidate switches as cluster members	GC
rcommand	Provides configuration access to Member switches	PE
show cluster	Displays the switch clustering status	PE
show cluster members	Displays current cluster Members	PE
show cluster candidates	Displays current cluster Candidates in the network	PE

Using Switch Clustering

- ◆ A switch cluster has a primary unit called the “Commander” which is used to manage all other “Member” switches in the cluster. The management station can use either Telnet or the web interface to communicate directly with the

Commander through its IP address, and then use the Commander to manage the Member switches through the cluster's "internal" IP addresses.

- ◆ Clustered switches must be in the same Ethernet broadcast domain. In other words, clustering only functions for switches which can pass information between the Commander and potential Candidates or active Members through VLAN 4093.
- ◆ Once a switch has been configured to be a cluster Commander, it automatically discovers other cluster-enabled switches in the network. These "Candidate" switches only become cluster Members when manually selected by the administrator through the management station.



Note: Cluster Member switches can be managed either through a Telnet connection to the Commander, or through a web management connection to the Commander. When using a console connection, from the Commander CLI prompt, use the **command** to connect to the Member switch.

cluster This command enables clustering on the switch. Use the **no** form to disable clustering.

Syntax

[no] cluster

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ To create a switch cluster, first be sure that clustering is enabled on the switch (the default is enabled), then set the switch as a Cluster Commander. Set a Cluster IP Pool that does not conflict with any other IP subnets in the network. Cluster IP addresses are assigned to switches when they become Members and are used for communication between Member switches and the Commander.
- ◆ Switch clusters are limited to the same Ethernet broadcast domain.
- ◆ There can be up to 100 candidates and 16 member switches in one cluster.
- ◆ A switch can only be a Member of one cluster.
- ◆ Configured switch clusters are maintained across power resets and network changes.

Example

```
Console(config)#cluster
Console(config)#
```

cluster commander This command enables the switch as a cluster Commander. Use the **no** form to disable the switch as cluster Commander.

Syntax

[no] cluster commander

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ Once a switch has been configured to be a cluster Commander, it automatically discovers other cluster-enabled switches in the network. These “Candidate” switches only become cluster Members when manually selected by the administrator through the management station.
- ◆ Cluster Member switches can be managed through a Telnet connection to the Commander. From the Commander CLI prompt, use the [rcommand id](#) command to connect to the Member switch.

Example

```
Console(config)#cluster commander
Console(config)#
```

cluster ip-pool This command sets the cluster IP address pool. Use the **no** form to reset to the default address.

Syntax

cluster ip-pool *ip-address*

no cluster ip-pool

ip-address - The base IP address for IP addresses assigned to cluster Members. The IP address must start 10.x.x.x.

Default Setting

10.254.254.1

Command Mode

Global Configuration

Command Usage

- ◆ An “internal” IP address pool is used to assign IP addresses to Member switches in the cluster. Internal cluster IP addresses are in the form 10.x.x.member-ID. Only the base IP address of the pool needs to be set since Member IDs can only be between 1 and 36.
- ◆ Set a Cluster IP Pool that does not conflict with addresses in the network IP subnet. Cluster IP addresses are assigned to switches when they become Members and are used for communication between Member switches and the Commander.
- ◆ You cannot change the cluster IP pool when the switch is currently in Commander mode. Commander mode must first be disabled.

Example

```
Console(config)#cluster ip-pool 10.2.3.4  
Console(config)#
```

cluster member This command configures a Candidate switch as a cluster Member. Use the **no** form to remove a Member switch from the cluster.

Syntax

cluster member mac-address *mac-address* **id** *member-id*

no cluster member id *member-id*

mac-address - The MAC address of the Candidate switch.

member-id - The ID number to assign to the Member switch. (Range: 1-16)

Default Setting

No Members

Command Mode

Global Configuration

Command Usage

- ◆ The maximum number of cluster Members is 16.
- ◆ The maximum number of cluster Candidates is 100.

Example

```
Console(config)#cluster member mac-address 00-12-34-56-78-9a id 5  
Console(config)#
```

rcommand This command provides access to a cluster Member CLI for configuration.

Syntax

rcommand id *member-id*

member-id - The ID number of the Member switch. (Range: 1-16)

Command Mode

Privileged Exec

Command Usage

- ◆ This command only operates through a Telnet connection to the Commander switch. Managing cluster Members using the local console CLI on the Commander is not supported.
- ◆ There is no need to enter the username and password for access to the Member switch CLI.

Example

```
Console#rcommand id 1

CLI session with the ECS5610-52S is opened.
To end the CLI session, enter [Exit].

Vty-0#
```

show cluster This command shows the switch clustering configuration.

Command Mode

Privileged Exec

Example

```
Console#show cluster
Role                : commander
Interval Heartbeat  : 30
Heartbeat Loss Count : 3 seconds
Number of Members   : 1
Number of Candidates : 2
Console#
```


show cluster members This command shows the current switch cluster members.

Command Mode

Privileged Exec

Example

```
Console#show cluster members
Cluster Members:
ID          : 1
Role        : Active member
IP Address  : 10.254.254.2
MAC Address : 00-E0-0C-00-00-FE
Description : ECS5610-52S
Console#
```

show cluster candidates This command shows the discovered Candidate switches in the network.

Command Mode

Privileged Exec

Example

```
Console#show cluster candidates
Cluster Candidates:
Role          MAC Address      Description
-----
Active member 00-E0-0C-00-00-FE ECS5610-52S
CANDIDATE     00-12-CF-0B-47-A0 ECS5610-52S
Console#
```


SNMP Commands

SNMP commands control access to this switch from management stations using the Simple Network Management Protocol (SNMP), as well as the error types sent to trap managers.

SNMP Version 3 also provides security features that cover message integrity, authentication, and encryption; as well as controlling user access to specific areas of the MIB tree. To use SNMPv3, first set an SNMP engine ID (or accept the default), specify read and write access views for the MIB tree, configure SNMP user groups with the required security model (i.e., SNMP v1, v2c or v3) and security level (i.e., authentication and privacy), and then assign SNMP users to these groups, along with their specific authentication and privacy passwords.

Table 28: SNMP Commands

Command	Function	Mode
<i>General SNMP Commands</i>		
<code>snmp-server</code>	Enables the SNMP agent	GC
<code>snmp-server community</code>	Sets up the community access string to permit access to SNMP commands	GC
<code>snmp-server contact</code>	Sets the system contact string	GC
<code>snmp-server location</code>	Sets the system location string	GC
<code>show snmp</code>	Displays the status of SNMP communications	NE, PE
<i>SNMP Target Host Commands</i>		
<code>snmp-server enable traps</code>	Enables the device to send SNMP traps (i.e., SNMP notifications)	GC
<code>snmp-server host</code>	Specifies the recipient of an SNMP notification operation	GC
<i>SNMPv3 Commands</i>		
<code>snmp-server engine-id</code>	Sets the SNMP engine ID	GC
<code>snmp-server group</code>	Adds an SNMP group, mapping users to views	GC
<code>snmp-server user</code>	Adds a user to an SNMP group	GC
<code>snmp-server view</code>	Adds an SNMP view	GC
<code>show snmp engine-id</code>	Shows the SNMP engine ID	PE
<code>show snmp group</code>	Shows the SNMP groups	PE
<code>show snmp user</code>	Shows the SNMP users	PE
<code>show snmp view</code>	Shows the SNMP views	PE

Table 28: SNMP Commands (Continued)

Command	Function	Mode
<i>Notification Log Commands</i>		
<code>nlm</code>	Enables the specified notification log	GC
<code>snmp-server notify-filter</code>	Creates a notification log and specifies the target host	GC
<code>show nlm oper-status</code>	Shows operation status of configured notification logs	PE
<code>show snmp notify-filter</code>	Displays the configured notification logs	PE
<i>ATC Trap Commands</i>		
<code>snmp-server enable port-traps atc broadcast-alarm-clear</code>	Sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered	IC (Port)
<code>snmp-server enable port-traps atc broadcast-alarm-fire</code>	Sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control	IC (Port)
<code>snmp-server enable port-traps atc broadcast-control-apply</code>	Sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control and the apply timer expires	IC (Port)
<code>snmp-server enable port-traps atc broadcast-control-release</code>	Sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires	IC (Port)
<code>snmp-server enable port-traps atc multicast-alarm-clear</code>	Sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered	IC (Port)
<code>snmp-server enable port-traps atc multicast-alarm-fire</code>	Sends a trap when multicast traffic exceeds the upper threshold for automatic storm control	IC (Port)
<code>snmp-server enable port-traps atc multicast-control-apply</code>	Sends a trap when multicast traffic exceeds the upper threshold for automatic storm control and the apply timer expires	IC (Port)
<code>snmp-server enable port-traps atc multicast-control-release</code>	Sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires	IC (Port)
<i>Transceiver Power Threshold Trap Commands</i>		
<code>transceiver-threshold current</code>	Sends a trap when the transceiver current falls outside the specified thresholds	IC (Port)
<code>transceiver-threshold rx-power</code>	Sends a trap when the power level of the received signal falls outside the specified thresholds	IC (Port)
<code>transceiver-threshold temperature</code>	Sends a trap when the transceiver temperature falls outside the specified thresholds	IC (Port)
<code>transceiver-threshold tx-power</code>	Sends a trap when the power level of the transmitted signal power outside the specified thresholds	IC (Port)
<code>transceiver-threshold voltage</code>	Sends a trap when the transceiver voltage falls outside the specified thresholds	IC (Port)
<i>Additional Trap Commands</i>		
<code>memory</code>	Sets the rising and falling threshold for the memory utilization alarm	GC
<code>process cpu</code>	Sets the rising and falling threshold for the CPU utilization alarm	GC

Table 28: SNMP Commands (Continued)

Command	Function	Mode
<code>show memory</code>	Shows memory utilization parameters	PE
<code>show process cpu</code>	Shows CPU utilization parameters	PE

General SNMP Commands

snmp-server This command enables the SNMPv3 engine and services for all management clients (i.e., versions 1, 2c, 3). Use the **no** form to disable the server.

Syntax

[no] snmp-server

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server
Console(config)#
```

snmp-server community This command defines community access strings used to authorize management access by clients using SNMP v1 or v2c. Use the **no** form to remove the specified community string.

Syntax

snmp-server community *string* [**ro** | **rw**]

no snmp-server community *string*

string - Community string that acts like a password and permits access to the SNMP protocol. (Maximum length: 32 characters, case sensitive; Maximum number of strings: 5)

ro - Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.

rw - Specifies read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Default Setting

- ◆ **public** - Read-only access. Authorized management stations are only able to retrieve MIB objects.

- ◆ private - Read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server community alpha rw
Console(config)#
```

snmp-server contact This command sets the system contact string. Use the **no** form to remove the system contact information.

Syntax

snmp-server contact *string*

no snmp-server contact

string - String that describes the system contact information.
(Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server contact Paul
Console(config)#
```

Related Commands

[snmp-server location \(182\)](#)

snmp-server location This command sets the system location string. Use the **no** form to remove the location string.

Syntax

snmp-server location *text*

no snmp-server location

text - String that describes the system location.
(Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server location WC-19
Console(config)#
```

Related Commands

[snmp-server contact \(182\)](#)

show snmp This command can be used to check the status of SNMP communications.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command provides information on the community access strings, counter information for SNMP input and output protocol data units, and whether or not SNMP logging has been enabled with the **snmp-server enable traps** command.

Example

```
Console#show snmp

SNMP Agent : Enabled

SNMP Traps :
  Authentication : Enabled
  Link-up-down   : Enabled

SNMP Communities :
  1. public, and the access level is read-only
  2. private, and the access level is read/write

0 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  0 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  0 Get-next PDUs
  0 Set-request PDUs
0 SNMP packets output
  0 Too big errors
  0 No such name errors
```

```
0 Bad values errors
0 General errors
0 Response PDUs
0 Trap PDUs
```

```
SNMP Logging: Disabled
Console#
```

SNMP Target Host Commands

snmp-server enable traps This command enables this device to send Simple Network Management Protocol traps or informs (i.e., SNMP notifications). Use the **no** form to disable SNMP notifications.

Syntax

[no] snmp-server enable traps [authentication | link-up-down]

authentication - Keyword to issue authentication failure notifications.

link-up-down - Keyword to issue link-up or link-down notifications.

Default Setting

Issue authentication and link-up-down traps.

Command Mode

Global Configuration

Command Usage

- ◆ If you do not enter an **snmp-server enable traps** command, no notifications controlled by this command are sent. In order to configure this device to send SNMP notifications, you must enter at least one **snmp-server enable traps** command. If you enter the command with no keywords, both authentication and link-up-down notifications are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled.
- ◆ The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host** command.
- ◆ The authentication, link-up, and link-down traps are legacy notifications, and therefore when used for SNMP Version 3 hosts, they must be enabled in conjunction with the corresponding entries in the Notify View assigned by the **snmp-server group** command.

Example

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```


Related Commands

[snmp-server host \(185\)](#)

snmp-server host This command specifies the recipient of a Simple Network Management Protocol notification operation. Use the **no** form to remove the specified host.

Syntax

snmp-server host *host-addr* [**inform** [**retry** *retries* | **timeout** *seconds*]]
community-string

[**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**] [**udp-port** *port*]}]

no snmp-server host *host-addr*

host-addr - IPv4 or IPv6 address of the host (targeted recipient).
(Maximum host addresses: 5 trap destination IP address entries)

inform - Notifications are sent as inform messages. Note that this option is only available for version 2c and 3 hosts. (Default: traps are used)

retries - The maximum number of times to resend an inform message if the recipient does not acknowledge receipt. (Range: 0-255; Default: 3)

seconds - The number of seconds to wait for an acknowledgment before resending an inform message. (Range: 0-2147483647 centiseconds; Default: 1500 centiseconds)

community-string - Password-like community string sent with the notification operation to SNMP V1 and V2c hosts. Although you can set this string using the **snmp-server host** command by itself, we recommend defining it with the [snmp-server community](#) command prior to using the **snmp-server host** command. (Maximum length: 32 characters)

version - Specifies whether to send notifications as SNMP Version 1, 2c or 3 traps. (Range: 1, 2c, 3; Default: 1)

auth | **noauth** | **priv** - This group uses SNMPv3 with authentication, no authentication, or with authentication and privacy. See "Simple Network Management Protocol" in the *Web Management Guide* for further information about these authentication and encryption options.

port - Host UDP port to use. (Range: 1-65535; Default: 162)

Default Setting

Host Address: None

Notification Type: Traps

SNMP Version: 1

UDP Port: 162

Command Mode

Global Configuration

Command Usage

- ◆ If you do not enter an **snmp-server host** command, no notifications are sent. In order to configure the switch to send SNMP notifications, you must enter at least one **snmp-server host** command. In order to enable multiple hosts, you must issue a separate **snmp-server host** command for each host.
- ◆ The **snmp-server host** command is used in conjunction with the **snmp-server enable traps** command. Use the **snmp-server enable traps** command to enable the sending of traps or informs and to specify which SNMP notifications are sent globally. For a host to receive notifications, at least one **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled.
- ◆ Some notification types cannot be controlled with the **snmp-server enable traps** command. For example, some notification types are always enabled.
- ◆ Notifications are issued by the switch as trap messages by default. The recipient of a trap message does not send a response to the switch. Traps are therefore not as reliable as inform messages, which include a request for acknowledgement of receipt. Informs can be used to ensure that critical information is received by the host. However, note that informs consume more system resources because they must be kept in memory until a response is received. Informs also add to network traffic. You should consider these effects when deciding whether to issue notifications as traps or informs.

To send an inform to a SNMPv2c host, complete these steps:

1. Enable the SNMP agent ([page 181](#)).
2. Create a view with the required notification messages ([page 191](#)).
3. Create a group that includes the required notify view ([page 188](#)).
4. Allow the switch to send SNMP traps; i.e., notifications ([page 184](#)).
5. Specify the target host that will receive inform messages with the **snmp-server host** command as described in this section.

To send an inform to a SNMPv3 host, complete these steps:

1. Enable the SNMP agent ([page 181](#)).
 2. Create a local SNMPv3 user to use in the message exchange process ([page 189](#)).
 3. Create a view with the required notification messages ([page 191](#)).
 4. Create a group that includes the required notify view ([page 188](#)).
 5. Allow the switch to send SNMP traps; i.e., notifications ([page 184](#)).
 6. Specify the target host that will receive inform messages with the **snmp-server host** command as described in this section.
- ◆ The switch can send SNMP Version 1, 2c or 3 notifications to a host IP address, depending on the SNMP version that the management station supports. If the **snmp-server host** command does not specify the SNMP version, the default is to send SNMP version 1 notifications.

- ◆ If you specify an SNMP Version 3 host, then the community string is interpreted as an SNMP user name. The user name must first be defined with the [snmp-server user](#) command. Otherwise, an SNMPv3 group will be automatically created by the **snmp-server host** command using the name of the specified community string, and default settings for the read, write, and notify view.

Example

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#
```

Related Commands

[snmp-server enable traps \(184\)](#)

SNMPv3 Commands

snmp-server engine-id This command configures an identification string for the SNMPv3 engine. Use the **no** form to restore the default.

Syntax

snmp-server engine-id {**local** | **remote** *ip-address*}} *engineid-string*

no snmp-server engine-id {**local** | **remote** *ip-address*}}

local - Specifies the SNMP engine on this switch.

remote - Specifies an SNMP engine on a remote device.

ip-address - The Internet address of the remote device.

engineid-string - String identifying the engine ID. (Range: 1-26 hexadecimal characters)

Default Setting

A unique engine ID is automatically generated by the switch based on its MAC address.

Command Mode

Global Configuration

Command Usage

- ◆ An SNMP engine is an independent SNMP agent that resides either on this switch or on a remote device. This engine protects against message replay, delay, and redirection. The engine ID is also used in combination with user passwords to generate the security keys for authenticating and encrypting SNMPv3 packets.
- ◆ A remote engine ID is required when using SNMPv3 informs. (See the [snmp-server host](#) command.) The remote engine ID is used to compute the security digest for authentication and encryption of packets passed between the switch

and a user on the remote host. SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent's SNMP engine ID before you can send proxy requests or informs to it.

- ◆ Trailing zeroes need not be entered to uniquely specify a engine ID. In other words, the value "0123456789" is equivalent to "0123456789" followed by 16 zeroes for a local engine ID.
- ◆ A local engine ID is automatically generated that is unique to the switch. This is referred to as the default engine ID. If the local engine ID is deleted or changed, all SNMP users will be cleared. You will need to reconfigure all existing users ([page 189](#)).

Example

```
Console(config)#snmp-server engine-id local 1234567890
Console(config)#snmp-server engineID remote 9876543210 192.168.1.19
Console(config)#
```

Related Commands

[snmp-server host \(185\)](#)

snmp-server group This command adds an SNMP group, mapping SNMP users to SNMP views. Use the **no** form to remove an SNMP group.

Syntax

snmp-server group *groupname* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}}
[**read** *readview*] [**write** *writeview*] [**notify** *notifyview*]

no snmp-server group *groupname*

groupname - Name of an SNMP group. (Range: 1-32 characters)

v1 | **v2c** | **v3** - Use SNMP version 1, 2c or 3.

auth | **noauth** | **priv** - This group uses SNMPv3 with authentication, no authentication, or with authentication and privacy. See "Simple Network Management Protocol" in the *Web Management Guide* for further information about these authentication and encryption options.

readview - Defines the view for read access. (1-32 characters)

writeview - Defines the view for write access. (1-32 characters)

notifyview - Defines the view for notifications. (1-32 characters)

Default Setting

Default groups: public¹ (read only), private² (read/write)
readview - Every object belonging to the Internet OID space (1).
writeview - Nothing is defined.
notifyview - Nothing is defined.

Command Mode

Global Configuration

Command Usage

- ◆ A group sets the access policy for the assigned users.
- ◆ When authentication is selected, the MD5 or SHA algorithm is used as specified in the [snmp-server user](#) command.
- ◆ When privacy is selected, the DES 56-bit algorithm is used for data encryption.
- ◆ For additional information on the notification messages supported by this switch, see the *Web Management Guide*. Also, note that the authentication, link-up and link-down messages are legacy traps and must therefore be enabled in conjunction with the [snmp-server enable traps](#) command.

Example

```
Console(config)#snmp-server group r&d v3 auth write daily
Console(config)#
```

snmp-server user This command adds a user to an SNMP group, restricting the user to a specific SNMP Read, Write, or Notify View. Use the **no** form to remove a user from an SNMP group.

Syntax

snmp-server user *username* *groupname* [**remote** *ip-address*]
 {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*
 [**priv** **des56** *priv-password*]]

no snmp-server user *username* {**v1** | **v2c** | **v3** | **remote**}

username - Name of user connecting to the SNMP agent.
 (Range: 1-32 characters)

groupname - Name of an SNMP group to which the user is assigned.
 (Range: 1-32 characters)

remote - Specifies an SNMP engine on a remote device.

ip-address - The Internet address of the remote device.

v1 | **v2c** | **v3** - Use SNMP version 1, 2c or 3.

1. No view is defined.
2. Maps to the defaultview.

encrypted - Accepts the password as encrypted input.

auth - Uses SNMPv3 with authentication.

md5 | sha - Uses MD5 or SHA authentication.

auth-password - Authentication password. Enter as plain text if the **encrypted** option is not used. Otherwise, enter an encrypted password. (A minimum of eight characters is required.)

priv des56 - Uses SNMPv3 with privacy with DES56 encryption.

priv-password - Privacy password. Enter as plain text if the **encrypted** option is not used. Otherwise, enter an encrypted password.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ Local users (i.e., the command does not specify a remote engine identifier) must be configured to authorize management access for SNMPv3 clients, or to identify the source of SNMPv3 trap messages sent from the local switch.
- ◆ Remote users (i.e., the command specifies a remote engine identifier) must be configured to identify the source of SNMPv3 inform messages sent from the local switch.
- ◆ The SNMP engine ID is used to compute the authentication/privacy digests from the password. You should therefore configure the engine ID with the [snmp-server engine-id](#) command before using this configuration command.
- ◆ Before you configure a remote user, use the [snmp-server engine-id](#) command to specify the engine ID for the remote device where the user resides. Then use the **snmp-server user** command to specify the user and the IP address for the remote device where the user resides. The remote agent's SNMP engine ID is used to compute authentication/privacy digests from the user's password. If the remote engine ID is not first configured, the **snmp-server user** command specifying a remote user will fail.
- ◆ SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent's SNMP engine ID before you can send proxy requests or informs to it.

Example

```
Console(config)#snmp-server user steve group r&d v3 auth md5 greenpeace priv  
des56 einstien  
Console(config)#snmp-server user mark group r&d remote 192.168.1.19 v3 auth  
md5 greenpeace priv des56 einstien  
Console(config)#
```

snmp-server view This command adds an SNMP view which controls user access to the MIB. Use the **no** form to remove an SNMP view.

Syntax

snmp-server view *view-name oid-tree* {**included** | **excluded**}

no snmp-server view *view-name*

view-name - Name of an SNMP view. (Range: 1-32 characters)

oid-tree - Object identifier of a branch within the MIB tree. Wild cards can be used to mask a specific portion of the OID string. (Refer to the examples.)

included - Defines an included view.

excluded - Defines an excluded view.

Default Setting

defaultview (includes access to the entire MIB tree)

Command Mode

Global Configuration

Command Usage

- ◆ Views are used in the [snmp-server group](#) command to restrict user access to specified portions of the MIB tree.
- ◆ The predefined view “defaultview” includes access to the entire MIB tree.

Examples

This view includes MIB-2.

```
Console(config)#snmp-server view mib-2 1.3.6.1.2.1 included  
Console(config)#
```

This view includes the MIB-2 interfaces table, ifDescr. The wild card is used to select all the index values in this table.

```
Console(config)#snmp-server view ifEntry.2 1.3.6.1.2.1.2.2.1.*.2 included  
Console(config)#
```

This view includes the MIB-2 interfaces table, and the mask selects all index entries.

```
Console(config)#snmp-server view ifEntry.a 1.3.6.1.2.1.2.2.1.1.* included
Console(config)#
```

show snmp engine-id This command shows the SNMP engine ID.

Command Mode

Privileged Exec

Example

This example shows the default engine ID.

```
Console#show snmp engine-id
Local SNMP EngineID: 8000002a8000000000e8666672
Local SNMP EngineBoots: 1

Remote SNMP EngineID                               IP address
80000000030004e2b316c54321                         192.168.1.19
Console#
```

Table 29: show snmp engine-id - display description

Field	Description
Local SNMP engineID	String identifying the engine ID.
Local SNMP engineBoots	The number of times that the engine has (re-)initialized since the snmp EngineID was last configured.
Remote SNMP engineID	String identifying an engine ID on a remote device.
IP address	IP address of the device containing the corresponding remote SNMP engine.

show snmp group Four default groups are provided – SNMPv1 read-only access and read/write access, and SNMPv2c read-only access and read/write access.

Command Mode

Privileged Exec

Example

```
Console#show snmp group
Group Name: r&d
Security Model: v3
Read View: defaultview
Write View: daily
Notify View: none
Storage Type: permanent
Row Status: active
```



```
Group Name: public
Security Model: v1
Read View: defaultview
Write View: none
Notify View: none
Storage Type: volatile
Row Status: active
```

```
Group Name: public
Security Model: v2c
Read View: defaultview
Write View: none
Notify View: none
Storage Type: volatile
Row Status: active
```

```
Group Name: private
Security Model: v1
Read View: defaultview
Write View: defaultview
Notify View: none
Storage Type: volatile
Row Status: active
```

```
Group Name: private
Security Model: v2c
Read View: defaultview
Write View: defaultview
Notify View: none
Storage Type: volatile
Row Status: active
```

Console#

Table 30: show snmp group - display description

Field	Description
groupname	Name of an SNMP group.
security model	The SNMP version.
readview	The associated read view.
writeview	The associated write view.
notifyview	The associated notify view.
storage-type	The storage type for this entry.
Row Status	The row status of this entry.

show snmp user This command shows information on SNMP users.

Command Mode
Privileged Exec

Example

```
Console#show snmp user
EngineId: 800000ca030030f1df9ca00000
User Name: steve
Authentication Protocol: md5
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active

SNMP remote user
EngineId: 80000000030004e2b316c54321
User Name: mark
Authentication Protocol: mdt
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active

Console#
```

Table 31: show snmp user - display description

Field	Description
EngineId	String identifying the engine ID.
User Name	Name of user connecting to the SNMP agent.
Authentication Protocol	The authentication protocol used with SNMPv3.
Privacy Protocol	The privacy protocol used with SNMPv3.
Storage Type	The storage type for this entry.
Row Status	The row status of this entry.
SNMP remote user	A user associated with an SNMP engine on a remote device.

show snmp view This command shows information on the SNMP views.

Command Mode
Privileged Exec

Example

```
Console#show snmp view
View Name: mib-2
Subtree OID: 1.2.2.3.6.2.1
View Type: included
Storage Type: permanent
Row Status: active
```

```
View Name: defaultview
Subtree OID: 1
View Type: included
Storage Type: volatile
Row Status: active
```

```
Console#
```

Table 32: show snmp view - display description

Field	Description
View Name	Name of an SNMP view.
Subtree OID	A branch in the MIB tree.
View Type	Indicates if the view is included or excluded.
Storage Type	The storage type for this entry.
Row Status	The row status of this entry.

Notification Log Commands

nlm This command enables or disables the specified notification log.

Syntax

[no] nlm *filter-name*

filter-name - Notification log name. (Range: 1-32 characters)

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

- ◆ Notification logging is enabled by default, but will not start recording information until a logging profile specified by the [snmp-server notify-filter](#) command is enabled by the **nlm** command.
- ◆ Disabling logging with this command does not delete the entries stored in the notification log.

Example

This example enables the notification log A1.

```
Console(config)#nlm A1
Console(config)#
```

snmp-server notify-filter This command creates an SNMP notification log. Use the **no** form to remove this log.

Syntax

[no] snmp-server notify-filter *profile-name* **remote** *ip-address*

profile-name - Notification log profile name. (Range: 1-32 characters)

ip-address - The Internet address of a remote device. The specified target host must already have been configured using the [snmp-server host](#) command.



Note: The notification log is stored locally. It is not sent to a remote device. This remote host parameter is only required to complete mandatory fields in the SNMP Notification MIB.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ Systems that support SNMP often need a mechanism for recording Notification information as a hedge against lost notifications, whether there are Traps or Informs that may be exceeding retransmission limits. The Notification Log MIB (NLM, RFC 3014) provides an infrastructure in which information from other MIBs may be logged.
- ◆ Given the service provided by the NLM, individual MIBs can now bear less responsibility to record transient information associated with an event against the possibility that the Notification message is lost, and applications can poll the log to verify that they have not missed any important Notifications.
- ◆ If notification logging is not configured and enabled, when the switch reboots, some SNMP traps (such as warm start) cannot be logged.
- ◆ To avoid this problem, notification logging should be configured and enabled using the **snmp-server notify-filter** command and [nlm](#) command, and these commands stored in the startup configuration file. Then when the switch reboots, SNMP traps (such as warm start) can now be logged.
- ◆ When this command is executed, a notification log is created (with the default parameters defined in RFC 3014). Notification logging is enabled by default (see the [nlm](#) command), but will not start recording information until a logging profile specified with this command is enabled with the [nlm](#) command.
- ◆ Based on the default settings used in RFC 3014, a notification log can contain up to 256 entries, and the entry aging time is 1440 minutes. Information

recorded in a notification log, and the entry aging time can only be configured using SNMP from a network management station.

- ◆ When a trap host is created with the `snmp-server host` command, a default notify filter will be created as shown in the example under the `show snmp notify-filter` command.

Example

This example first creates an entry for a remote host, and then instructs the switch to record this device as the remote host for the specified notification log.

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#snmp-server notify-filter A1 remote 10.1.19.23
Console#
```

show nlm oper-status This command shows the operational status of configured notification logs.

Command Mode

Privileged Exec

Example

```
Console#show nlm oper-status
Filter Name: A1
Oper-Status: Operational
Console#
```

show snmp notify-filter This command displays the configured notification logs.

Command Mode

Privileged Exec

Example

This example displays the configured notification logs and associated target hosts.

```
Console#show snmp notify-filter
Filter profile name      IP address
-----
A1                      10.1.19.23
Console#
```

Additional Trap Commands

memory This command sets an SNMP trap based on configured thresholds for memory utilization. Use the **no** form to restore the default setting.

Syntax

memory {**rising** *rising-threshold* | **falling** *falling-threshold*}

no memory {**rising** | **falling**}

rising-threshold - Rising threshold for memory utilization alarm expressed in percentage. (Range: 1-100)

falling-threshold - Falling threshold for memory utilization alarm expressed in percentage. (Range: 1-100)

Default Setting

Rising Threshold: 90%

Falling Threshold: 70%

Command Mode

Global Configuration

Command Usage

Once the rising alarm threshold is exceeded, utilization must drop beneath the falling threshold before the alarm is terminated, and then exceed the rising threshold again before another alarm is triggered.

Example

```
Console(config)#memory rising 80
Console(config)#memory falling 60
Console#
```

Related Commands

[show memory \(113\)](#)

process cpu This command sets an SNMP trap based on configured thresholds for CPU utilization. Use the **no** form to restore the default setting.

Syntax

process cpu {**rising** *rising-threshold* | **falling** *falling-threshold*}

no process cpu {**rising** | **falling**}

rising-threshold - Rising threshold for CPU utilization alarm expressed in percentage. (Range: 1-100)

falling-threshold - Falling threshold for CPU utilization alarm expressed in percentage. (Range: 1-100)

Default Setting

Rising Threshold: 90%

Falling Threshold: 70%

Command Mode

Global Configuration

Command Usage

Once the rising alarm threshold is exceeded, utilization must drop beneath the falling threshold before the alarm is terminated, and then exceed the rising threshold again before another alarm is triggered.

Example

```
Console(config)#process cpu rising 80
Console(config)#process cpu falling 60
Console#
```

Related Commands

[show process cpu \(114\)](#)

Remote Monitoring Commands

Remote Monitoring allows a remote device to collect information or respond to specified events on an independent basis. This switch is an RMON-capable device which can independently perform a wide range of tasks, significantly reducing network management traffic. It can continuously run diagnostics and log information on network performance. If an event is triggered, it can automatically notify the network administrator of a failure and provide historical information about the event. If it cannot connect to the management agent, it will continue to perform any specified tasks and pass data back to the management station the next time it is contacted.

This switch supports mini-RMON, which consists of the Statistics, History, Event and Alarm groups. When RMON is enabled, the system gradually builds up information about its physical interfaces, storing this information in the relevant RMON database group. A management agent then periodically communicates with the switch using the SNMP protocol. However, if the switch encounters a critical event, it can automatically send a trap message to the management agent which can then respond to the event if so configured.

Table 33: RMON Commands

Command	Function	Mode
<code>rmon alarm</code>	Sets threshold bounds for a monitored variable	GC
<code>rmon event</code>	Creates a response event for an alarm	GC
<code>rmon collection history</code>	Periodically samples statistics	IC
<code>rmon collection rmon1</code>	Enables statistics collection	IC
<code>show rmon alarms</code>	Shows the settings for all configured alarms	PE
<code>show rmon events</code>	Shows the settings for all configured events	PE
<code>show rmon history</code>	Shows the sampling parameters for each entry	PE
<code>show rmon statistics</code>	Shows the collected statistics	PE

rmon alarm This command sets threshold bounds for a monitored variable. Use the **no** form to remove an alarm.

Syntax

```
rmon alarm index variable interval {absolute | delta}
rising-threshold threshold [event-index]
falling-threshold threshold [event-index] [owner name]
no rmon alarm index
```

index – Index to this entry. (Range: 1-65535)

variable – The object identifier of the MIB variable to be sampled. Only variables of the type etherStatsEntry.n.n may be sampled. Note that etherStatsEntry.n uniquely defines the MIB variable, and etherStatsEntry.n.n defines the MIB variable, plus the etherStatsIndex. For example, 1.3.6.1.2.1.16.1.1.1.6.1 denotes etherStatsBroadcastPkts, plus the etherStatsIndex of 1.

interval – The polling interval. (Range: 1-31622400 seconds)

absolute – The variable is compared directly to the thresholds at the end of the sampling period.

delta – The last sample is subtracted from the current value and the difference is then compared to the thresholds.

threshold – An alarm threshold for the sampled variable.
(Range: 0-2147483647)

event-index – The index of the event to use if an alarm is triggered. If there is no corresponding entry in the event control table, then no event will be generated. (Range: 1-65535)

name – Name of the person who created this entry. (Range: 1-127 characters)

Default Setting

1.3.6.1.2.1.16.1.1.1.6.1 - 1.3.6.1.2.1.16.1.1.1.6.1-52

Taking delta samples every 30 seconds,

Rising threshold is 892800, assigned to event 0

Falling threshold is 446400, assigned to event 0

Command Mode

Global Configuration

Command Usage

- ◆ If an event is already defined for an index, the entry must be deleted before any changes can be made with this command.
- ◆ If the current value is greater than or equal to the rising threshold, and the last sample value was less than this threshold, then an alarm will be generated. After a rising event has been generated, another such event will not be

generated until the sampled value has fallen below the rising threshold, reaches the falling threshold, and again moves back up to the rising threshold.

- ◆ If the current value is less than or equal to the falling threshold, and the last sample value was greater than this threshold, then an alarm will be generated. After a falling event has been generated, another such event will not be generated until the sampled value has risen above the falling threshold, reaches the rising threshold, and again moves back down to the failing threshold.

Example

```
Console(config)#rmon alarm 1 1.3.6.1.2.1.16.1.1.1.6.1 15 delta
    rising-threshold 100 1 falling-threshold 30 1 owner mike
Console(config)#
```

rmon event This command creates a response event for an alarm. Use the **no** form to remove an event.

Syntax

rmon event *index* [**log**] | [**trap** *community*] | [**description** *string*] | [**owner** *name*]

no rmon event *index*

index – Index to this entry. (Range: 1-65535)

log – Generates an RMON log entry when the event is triggered. Log messages are processed based on the current configuration settings for event logging (see [“Event Logging” on page 145](#)).

trap – Sends a trap message to all configured trap managers (see [“snmp-server host” on page 185](#)).

community – A password-like community string sent with the trap operation to SNMP v1 and v2c hosts. Although this string can be set using the **rmon event** command by itself, it is recommended that the string be defined using the [snmp-server community](#) command prior to using the **rmon event** command. (Range: 1-32 characters)

string – A comment that describes this event. (Range: 1-127 characters)

name – Name of the person who created this entry.
(Range: 1-127 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ If an event is already defined for an index, the entry must be deleted before any changes can be made with this command.
- ◆ The specified events determine the action to take when an alarm triggers this event. The response to an alarm can include logging the alarm or sending a message to a trap manager.

Example

```
Console(config)#rmon event 2 log description urgent owner mike
Console(config)#
```

rmon collection history This command periodically samples statistics on a physical interface. Use the **no** form to disable periodic sampling.

Syntax

rmon collection history controlEntry *index*

[**buckets** *number* [**interval** *seconds*]] | [**interval** *seconds*] |
[**owner** *name* [**buckets** *number* [**interval** *seconds*]]]

no rmon collection history controlEntry *index*

index – Index to this entry. (Range: 1-65535)

number – The number of buckets requested for this entry. (Range: 1-65536)

seconds – The polling interval. (Range: 1-3600 seconds)

name – Name of the person who created this entry.
(Range: 1-127 characters)

Default Setting

1.3.6.1.2.1.16.1.1.1.6.1 - 1.3.6.1.2.1.16.1.1.1.6.52

Buckets: 50

Interval: 30 seconds for even numbered entries,
1800 seconds for odd numbered entries

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ By default, each index number equates to a port on the switch, but can be changed to any number not currently in use.
- ◆ If periodic sampling is already enabled on an interface, the entry must be deleted before any changes can be made with this command.

- ◆ The information collected for each sample includes:
input octets, packets, broadcast packets, multicast packets, undersize packets, oversize packets, fragments, jabbers, CRC alignment errors, collisions, drop events, and network utilization.
- ◆ The switch reserves two controlEntry index entries for each port. If a default index entry is re-assigned to another port by this command, the **show running-config** command will display a message indicating that this index is not available for the port to which is normally assigned.

For example, if control entry 15 is assigned to port 5 as shown below, the **show running-config** command will indicate that this entry is not available for port 8.

```
Console(config)#interface ethernet 1/5
Console(config-if)#rmon collection history controlEntry 15
Console(config-if)#end
Console#show running-config
!
interface ethernet 1/5
  rmon collection history controlEntry 15 buckets 50 interval 1800
...
interface ethernet 1/8
  no rmon collection history controlEntry 15
```

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#rmon collection history controlentry 21 buckets 24
  interval 60 owner mike
Console(config-if)#
```

rmon collection rmon1 This command enables the collection of statistics on a physical interface. Use the **no rmon collection rmon1** to disable statistics collection.

Syntax

rmon collection rmon1 controlEntry *index* [**owner** *name*]

no rmon collection rmon1 controlEntry *index*

index – Index to this entry. (Range: 1-65535)

name – Name of the person who created this entry.
(Range: 1-127 characters)

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ By default, each index number equates to a port on the switch, but can be changed to any number not currently in use.
- ◆ If statistics collection is already enabled on an interface, the entry must be deleted before any changes can be made with this command.
- ◆ The information collected for each entry includes:
input octets, packets, broadcast packets, multicast packets, undersize packets, oversize packets, fragments, jabbers, CRC alignment errors, collisions, drop events, and packets of specified lengths

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#rmon collection rmon1 controlEntry 1 owner mike
Console(config-if)#
```

show rmon alarms This command shows the settings for all configured alarms.

Command Mode

Privileged Exec

Example

```
Console#show rmon alarms
Alarm 1 is valid, owned by
Monitors 1.3.6.1.2.1.16.1.1.1.6.1 every 30 seconds
Taking delta samples, last value was 0
Rising threshold is 892800, assigned to event 0
Falling threshold is 446400, assigned to event 0
:
```

show rmon events This command shows the settings for all configured events.

Command Mode

Privileged Exec

Example

```
Console#show rmon events
Event 2 is valid, owned by mike
Description is urgent
Event firing causes log and trap to community , last fired 00:00:00
Console#
```

show rmon history This command shows the sampling parameters configured for each entry in the history group.

Command Mode

Privileged Exec

Example

```
Console#show rmon history
Entry 1 is valid, and owned by
Monitors 1.3.6.1.2.1.2.2.1.1.1 every 1800 seconds
Requested # of time intervals, ie buckets, is 8
Granted # of time intervals, ie buckets, is 8
Sample # 1 began measuring at 00:00:01
Received 77671 octets, 1077 packets,
61 broadcast and 978 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers packets,
0 CRC alignment errors and 0 collisions.
# of dropped packet events is 0
Network utilization is estimated at 0
:
```

show rmon statistics This command shows the information collected for all configured entries in the statistics group.

Command Mode

Privileged Exec

Example

```
Console#show rmon statistics
Interface 1 is valid, and owned by
Monitors 1.3.6.1.2.1.2.2.1.1.1 which has
Received 164289 octets, 2372 packets,
120 broadcast and 2211 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions.
# of dropped packet events (due to lack of resources): 0
# of packets received of length (in octets):
64: 2245, 65-127: 87, 128-255: 31,
256-511: 5, 512-1023: 2, 1024-1518: 2
:
```


Flow Sampling Commands

Flow sampling (sFlow) can be used with a remote sFlow Collector to provide an accurate, detailed and real-time overview of the types and levels of traffic present on the network. The sFlow Agent samples 1 out of n packets from all data traversing the switch, re-encapsulates the samples as sFlow datagrams and transmits them to the sFlow Collector. This sampling occurs at the internal hardware level where all traffic is seen, whereas traditional probes only have a partial view of traffic as it is sampled at the monitored interface. Moreover, the processor and memory load imposed by the sFlow agent is minimal since local analysis does not take place.

Table 34: sFlow Commands

Command	Function	Mode
<code>sflow</code>	Enables sFlow globally for the switch	GC
<code>sflow destination</code>	Configures the IP address and UDP port used by the Collector	IC
<code>sflow max-datagram-size</code>	Configures the maximum size of the sFlow datagram payload	IC
<code>sflow max-header-size</code>	Configures the maximum size of the sFlow datagram header	IC
<code>sflow owner</code>	Configures the name of the receiver	IC
<code>sflow polling-interval</code>	Configures the interval at which counters are added to the sample datagram	IC
<code>sflow sample</code>	Configures the packet sampling rate	IC
<code>sflow source</code>	Enables sFlow on the source ports to be monitored	IC
<code>sflow timeout</code>	Configures the length of time samples are sent to the Collector before resetting all sFlow port parameters	IC
<code>show sflow</code>	Shows the global and interface settings for the sFlow process	PE

sflow This command enables sFlow globally for the switch. Use the **no** form to disable this feature.

Syntax

[no] sflow

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

Flow sampling must be enabled globally on the switch, as well as for those ports where it is required (see the [sflow source](#) command).

Example

```
Console(config)#sflow
Console(config)#
```

sflow destination This command configures the IP address and UDP port used by the Collector. Use the **no** form to restore the default settings.

Syntax

sflow destination {**ipv4** *ipv4-address* | **ipv6** *ipv6-address*} [*destination-udp-port*]

no sflow destination

ipv4-address - IPv4 address of the sFlow Collector. Valid IPv4 addresses consist of four decimal numbers, 0 to 255, separated by periods.

ipv6-address - IPv6 address of the sFlow Collector. A full IPv6 address including the network prefix and host address bits. An IPv6 address consists of 8 colon-separated 16-bit hexadecimal values. One double colon may be used to indicate the appropriate number of zeros required to fill the undefined fields.

destination-udp-port - The UDP port on which the Collector is listening for sFlow streams. (Range: 0-65534)

Default Setting

IP Address: null

UDP Port: 6343

Command Mode

Interface Configuration (Ethernet)

Example

This example configures the Collector's IP address, and uses the default UDP port.

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow destination ipv4 192.168.0.4
Console(config-if)#
```

sflow max-datagram-size This command configures the maximum size of the sFlow datagram payload. Use the **no** form to restore the default setting.

Syntax

sflow max-datagram-size *max-datagram-size*

no max-datagram-size

max-datagram-size - The maximum size of the sFlow datagram payload.
(Range: 200-1500 bytes)

Default Setting

1400 bytes

Command Mode

Interface Configuration (Ethernet)

Example

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow max-datagram-size 1500
Console(config-if)#
```

sflow max-header-size This command configures the maximum size of the sFlow datagram header. Use the **no** form to restore the default setting.

Syntax

sflow max-header-size *max-header-size*

no max-header-size

max-header-size - The maximum size of the sFlow datagram header.
(Range: 64-256 bytes)

Default Setting

128 bytes

Command Mode

Interface Configuration (Ethernet)

Example

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow max-header-size 256
Console(config-if)#
```

sflow owner This command configures the name of the receiver (i.e., sFlow Collector). Use the **no** form to remove this name.

Syntax

sflow owner *name*

no sflow owner

name - The name of the receiver. (Range: 1-256 characters)

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Example

This example set the owner's name to Lamar.

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow owner Lamar
Console(config-if)#
```

sflow polling-interval This command configures the interval at which counters are added to the sample datagram. Use the **no** form to restore the default polling interval.

Syntax

sflow polling-interval *seconds*

no sflow polling-interval

seconds - The interval at which the sFlow process adds counter values to the sample datagram. (Range: 0-10000000 seconds, where 0 disables this feature)

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Example

This example sets the polling interval to 10 seconds.

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow polling-interval 10
Console(config-if)#
```

sflow sample This command configures the packet sampling rate. Use the **no** form to restore the default rate.

Syntax

sflow sample *rate*

no sflow sample

rate - The packet sampling rate, or the number of packets out of which one sample will be taken. (Range: 256-16777215 packets)

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Example

This example sets the sample rate to 1 out of every 100 packets.

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow sample 100
Console(config-if)#
```

sflow source This command enables sFlow on the source ports to be monitored. Use the **no** form to disable sFlow on the specified ports.

Syntax

[no] sflow source

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Example

This example enables flow control on ports 9 through 16.

```
Console(config)#interface ethernet 1/9-16
Console(config-if)#sflow source
Console(config-if)#
```

sflow timeout This command configures the length of time samples are sent to the Collector before resetting all sFlow port parameters. Use the **no** form to restore the default time out.

Syntax

sflow timeout *seconds*

no sflow timeout

seconds - The length of time the sFlow process continuously sends samples to the Collector before resetting all sFlow port parameters.

(Range: 0-10000000 seconds, where 0 indicates no time out)

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

The sFlow agent sends sample data to an sFlow collector until the timeout set by this command expires. The sFlow agent then resets the sampling interval, the receiver's name, address and UDP port, the time out, maximum header size, and maximum datagram size.

Example

This example sets the time out to 1000 seconds.

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow timeout 10000
Console(config-if)#
```

show sflow This command shows the global and interface settings for the sFlow process.

Syntax

show sflow [**interface** *interface*]

interface

ethernet *unit/port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-52)

Command Mode

Privileged Exec

Example

```
Console#show sflow interface ethernet 1/9
```

```
Interface of Ethernet 1/9 :
  Interface status      : Enabled
  Owner name           : Lamar
  Owner destination     : 192.168.0.4
  Owner socket port    : 6343
  Time out             : 9994
  Maximum header size  : 256
  Maximum datagram size : 1500
  Sample rate          : 1/256
  Polling interval     : 10
```

```
Console#
```


Authentication Commands

You can configure this switch to authenticate users logging into the system for management access using local or remote authentication methods. Port-based authentication using IEEE 802.1X can also be configured to control either management access to the uplink ports or client access³ to the data ports.

Table 35: Authentication Commands

Command Group	Function
User Accounts	Configures the basic user names and passwords for management access
Authentication Sequence	Defines logon authentication method and precedence
RADIUS Client	Configures settings for authentication via a RADIUS server
TACACS+ Client	Configures settings for authentication via a TACACS+ server
AAA	Configures authentication, authorization, and accounting for network access
Web Server	Enables management access via a web browser
Telnet Server	Enables management access via Telnet
Secure Shell	Provides secure replacement for Telnet
802.1X Port Authentication	Configures host authentication on specific ports using 802.1X
Management IP Filter	Configures IP addresses that are allowed management access
PPPoE Intermediate Agent	Configures relay parameters required for sending authentication messages between a client and broadband remote access servers

3. For other methods of controlling client access, see [“General Security Measures” on page 275](#).

User Accounts

The basic commands required for management access are listed in this section. This switch also includes other options for password checking via the console or a Telnet connection (page 134), user authentication via a remote authentication server (page 217), and host access authentication for specific ports (page 253).

Table 36: User Access Commands

Command	Function	Mode
<code>enable password</code>	Sets a password to control access to the Privileged Exec level	GC
<code>username</code>	Establishes a user name-based authentication system at login	GC

enable password After initially logging onto the system, you should set the Privileged Exec password. Remember to record it in a safe place. This command controls access to the Privileged Exec level from the Normal Exec level. Use the **no** form to reset the default password.

Syntax

enable password [*level level*] {**0** | **7**} *password*

no enable password [*level level*]

level level - Level 15 for Privileged Exec. (Levels 0-14 are not used.)

{**0** | **7**} - 0 means plain password, 7 means encrypted password.

password - Password for this privilege level. (Maximum length: 32 characters plain text or encrypted, case sensitive)

Default Setting

The default is level 15.

The default password is "super"

Command Mode

Global Configuration

Command Usage

- ◆ You cannot set a null password. You will have to enter a password to change the command mode from Normal Exec to Privileged Exec with the `enable` command.
- ◆ The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from an FTP server. There is no need for you to manually configure encrypted passwords.

Example

```
Console(config)#enable password level 15 0 admin
Console(config)#
```

Related Commands

- [enable \(95\)](#)
- [authentication enable \(220\)](#)

username This command adds named users, requires authentication at login, specifies or changes a user's password (or specify that no password is required), or specifies or changes a user's access level. Use the **no** form to remove a user name.

Syntax

username *name* {**access-level** *level* | **nopassword** | **password** {**0** | **7**} *password*}

no username *name*

name - The name of the user. (Maximum length: 32 characters, case sensitive. Maximum users: 16)

access-level *level* - Specifies the user level.
The device has two predefined privilege levels:
0: Normal Exec, **15**: Privileged Exec.

nopassword - No password is required for this user to log in.

{**0** | **7**} - **0** means plain password, **7** means encrypted password.

password *password* - The authentication password for the user. (Maximum length: 32 characters plain text or encrypted, case sensitive)

Default Setting

The default access level is Normal Exec.
The factory defaults for the user names and passwords are:

Table 37: Default Login Settings

username	access-level	password
guest	0	guest
admin	15	admin

Command Mode

Global Configuration

Command Usage

The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from an FTP server. There is no need for you to manually configure encrypted passwords.

Example

This example shows how to set the access level and password for a user.

```
Console(config)#username bob access-level 15
Console(config)#username bob password 0 smith
Console(config)#
```

Authentication Sequence

Three authentication methods can be specified to authenticate users logging into the system for management access. The commands in this section can be used to define the authentication method and sequence.

Table 38: Authentication Sequence Commands

Command	Function	Mode
authentication enable	Defines the authentication method and precedence for command mode change	GC
authentication login	Defines logon authentication method and precedence	GC

authentication enable This command defines the authentication method and precedence to use when changing from Exec command mode to Privileged Exec command mode with the [enable](#) command. Use the **no** form to restore the default.

Syntax

authentication enable {[local] [radius] [tacacs]}

no authentication enable

local - Use local password only.

radius - Use RADIUS server password only.

tacacs - Use TACACS server password.

Default Setting

Local

Command Mode

Global Configuration

Command Usage

- ◆ RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.

- ◆ RADIUS and TACACS+ logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.
- ◆ You can specify three authentication methods in a single command to indicate the authentication sequence. For example, if you enter “**authentication enable radius tacacs local**,” the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted on the TACACS+ server. If the TACACS+ server is not available, the local user name and password is checked.

Example

```
Console(config)#authentication enable radius  
Console(config)#
```

Related Commands

enable password - sets the password for changing command modes (218)

authentication login This command defines the login authentication method and precedence. Use the **no** form to restore the default.

Syntax

authentication login {[**local**] [**radius**] [**tacacs**]}

no authentication login

local - Use local password.

radius - Use RADIUS server password.

tacacs - Use TACACS server password.

Default Setting

Local

Command Mode

Global Configuration

Command Usage

- ◆ RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.
- ◆ RADIUS and TACACS+ logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.

- ◆ You can specify three authentication methods in a single command to indicate the authentication sequence. For example, if you enter “**authentication login radius tacacs local**,” the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted on the TACACS+ server. If the TACACS+ server is not available, the local user name and password is checked.

Example

```
Console(config)#authentication login radius
Console(config)#
```

Related Commands

[username](#) - for setting the local user names and passwords (219)

RADIUS Client

Remote Authentication Dial-in User Service (RADIUS) is a logon authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch.

Table 39: RADIUS Client Commands

Command	Function	Mode
radius-server acct-port	Sets the RADIUS server network port	GC
radius-server auth-port	Sets the RADIUS server network port	GC
radius-server host	Specifies the RADIUS server	GC
radius-server key	Sets the RADIUS encryption key	GC
radius-server retransmit	Sets the number of retries	GC
radius-server timeout	Sets the interval between sending authentication requests	GC
show radius-server	Shows the current RADIUS settings	PE

radius-server acct-port This command sets the RADIUS server network port for accounting messages. Use the **no** form to restore the default.

Syntax

radius-server acct-port *port-number*

no radius-server acct-port

port-number - RADIUS server UDP port used for accounting messages.
(Range: 1-65535)

Default Setting

1813

Command Mode

Global Configuration

Example

```
Console(config)#radius-server acct-port 181
Console(config)#
```

radius-server acct-port This command sets the RADIUS server network port. Use the **no** form to restore the default.

Syntax

radius-server acct-port *port-number*

no radius-server acct-port

port-number - RADIUS server UDP port used for authentication messages.
(Range: 1-65535)

Default Setting

1812

Command Mode

Global Configuration

Example

```
Console(config)#radius-server auth-port 181
Console(config)#
```

radius-server host This command specifies primary and backup RADIUS servers, and authentication and accounting parameters that apply to each server. Use the **no** form to remove a specified server, or to restore the default values.

Syntax

**[no] radius-server index host host-ip-address [acct-port acct-port]
[auth-port auth-port] [key key] [retransmit retransmit] [timeout timeout]**

index - Allows you to specify up to five servers. These servers are queried in sequence until a server responds or the retransmit period expires.

host-ip-address - IP address of server.

acct-port - RADIUS server UDP port used for accounting messages.
(Range: 1-65535)

auth-port - RADIUS server UDP port used for authentication messages. (Range: 1-65535)

key - Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 48 characters)

retransmit - Number of times the switch will try to authenticate logon access via the RADIUS server. (Range: 1-30)

timeout - Number of seconds the switch waits for a reply before resending a request. (Range: 1-65535)

Default Setting

auth-port - 1812

acct-port - 1813

timeout - 5 seconds

retransmit - 2

Command Mode

Global Configuration

Example

```
Console(config)#radius-server 1 host 192.168.1.20 port 181 timeout 10
retransmit 5 key green
Console(config)#
```

radius-server key This command sets the RADIUS encryption key. Use the **no** form to restore the default.

Syntax

radius-server key *key-string*

no radius-server key

key-string - Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 48 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#radius-server key green
Console(config)#
```


radius-server retransmit This command sets the number of retries. Use the **no** form to restore the default.

Syntax

radius-server retransmit *number-of-retries*

no radius-server retransmit

number-of-retries - Number of times the switch will try to authenticate logon access via the RADIUS server. (Range: 1 - 30)

Default Setting

2

Command Mode

Global Configuration

Example

```
Console(config)#radius-server retransmit 5  
Console(config)#
```

radius-server timeout This command sets the interval between transmitting authentication requests to the RADIUS server. Use the **no** form to restore the default.

Syntax

radius-server timeout *number-of-seconds*

no radius-server timeout

number-of-seconds - Number of seconds the switch waits for a reply before resending a request. (Range: 1-65535)

Default Setting

5

Command Mode

Global Configuration

Example

```
Console(config)#radius-server timeout 10  
Console(config)#
```

show radius-server This command displays the current settings for the RADIUS server.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show radius-server

Remote RADIUS Server Configuration:

Global Settings:
Authentication Port Number : 1812
Accounting Port Number    : 1813
Retransmit Times          : 2
Request Timeout           : 5

Server 1:
Server IP Address         : 192.168.1.1
Authentication Port Number : 1812
Accounting Port Number    : 1813
Retransmit Times          : 2
Request Timeout           : 5

RADIUS Server Group:
Group Name                Member Index
-----
radius                    1
Console#
```

TACACS+ Client

Terminal Access Controller Access Control System (TACACS+) is a logon authentication protocol that uses software running on a central server to control access to TACACS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch.

Table 40: TACACS+ Client Commands

Command	Function	Mode
tacacs-server host	Specifies the TACACS+ server and optional parameters	GC
tacacs-server key	Sets the TACACS+ encryption key	GC
tacacs-server port	Specifies the TACACS+ server network port	GC
tacacs-server retransmit	Sets the number of retries	GC
tacacs-server timeout	Sets the interval between sending authentication requests	GC
show tacacs-server	Shows the current TACACS+ settings	GC

tacacs-server host This command specifies the TACACS+ server and other optional parameters. Use the **no** form to remove the server, or to restore the default values.

Syntax

tacacs-server *index* **host** *host-ip-address* [**key** *key*] [**port** *port-number*]
[**retransmit** *retransmit*] [**timeout** *timeout*]

no tacacs-server *index*

index - The index for this server. (Range: 1)

host-ip-address - IP address of a TACACS+ server.

key - Encryption key used to authenticate logon access for the client. Do not use blank spaces in the string. (Maximum length: 48 characters)

port-number - TACACS+ server TCP port used for authentication messages. (Range: 1-65535)

retransmit - Number of times the switch will try to authenticate logon access via the TACACS+ server. (Range: 1-30)

timeout - Number of seconds the switch waits for a reply before resending a request. (Range: 1-540)

Default Setting

authentication port - 49

timeout - 5 seconds

retransmit - 2

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server 1 host 192.168.1.25 port 181 timeout 10
retransmit 5 key green
Console(config)#
```

tacacs-server key This command sets the TACACS+ encryption key. Use the **no** form to restore the default.

Syntax

tacacs-server **key** *key-string*

no tacacs-server **key**

key-string - Encryption key used to authenticate logon access for the client. Do not use blank spaces in the string. (Maximum length: 48 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server key green
Console(config)#
```

tacacs-server port This command specifies the TACACS+ server network port. Use the **no** form to restore the default.

Syntax

tacacs-server port *port-number*

no tacacs-server port

port-number - TACACS+ server TCP port used for authentication messages.
(Range: 1-65535)

Default Setting

49

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server port 181
Console(config)#
```

tacacs-server retransmit This command sets the number of retries. Use the **no** form to restore the default.

Syntax

tacacs-server retransmit *number-of-retries*

no tacacs-server retransmit

number-of-retries - Number of times the switch will try to authenticate
logon access via the TACACS+ server. (Range: 1 - 30)

Default Setting

2

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server retransmit 5
Console(config)#
```

tacacs-server timeout This command sets the interval between transmitting authentication requests to the TACACS+ server. Use the **no** form to restore the default.

Syntax

tacacs-server timeout *number-of-seconds*

no tacacs-server timeout

number-of-seconds - Number of seconds the switch waits for a reply before resending a request. (Range: 1-540)

Default Setting

5

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server timeout 10
Console(config)#
```

show tacacs-server This command displays the current settings for the TACACS+ server.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show tacacs-server

Remote TACACS+ Server Configuration:

Global Settings:
  Server Port Number : 49
  Retransmit Times   : 2
  Timeout            : 5

Server 1:
  Server IP Address  : 10.11.12.13
  Server Port Number : 49
  Retransmit Times   : 2
  Timeout            : 4
```

```
TACACS+ Server Group:
Group Name                Member Index
-----
tacacs+                   1

Console#
```

AAA

The Authentication, Authorization, and Accounting (AAA) feature provides the main framework for configuring access control on the switch. The AAA functions require the use of configured RADIUS or TACACS+ servers in the network.

Table 41: AAA Commands

Command	Function	Mode
<code>aaa accounting dot1x</code>	Enables accounting of 802.1X services	GC
<code>aaa accounting exec</code>	Enables accounting of Exec services	GC
<code>aaa accounting update</code>	Enables periodoc updates to be sent to the accounting server	GC
<code>aaa authorization exec</code>	Enables authorization of Exec sessions	GC
<code>aaa group server</code>	Groups security servers in to defined lists	GC
<code>server</code>	Configures the IP address of a server in a group list	SG
<code>accounting dot1x</code>	Applies an accounting method to an interface for 802.1X service requests	IC
<code>accounting exec</code>	Applies an accounting method to local console, Telnet or SSH connections	Line
<code>authorization exec</code>	Applies an authorization method to local console, Telnet or SSH connections	Line
<code>show accounting</code>	Displays all accounting information	PE

aaa accounting dot1x This command enables the accounting of requested 802.1X services for network access. Use the **no** form to disable the accounting service.

Syntax

```
aaa accounting dot1x {default | method-name}
start-stop group {radius | tacacs+ | server-group}
no aaa accounting dot1x {default | method-name}
```

default - Specifies the default accounting method for service requests.

method-name - Specifies an accounting method for service requests.
(Range: 1-64 characters)

start-stop - Records accounting from starting point and stopping point.

group - Specifies the server group to use.

radius - Specifies all RADIUS hosts configure with the [radius-server host](#) command.

tacacs+ - Specifies all TACACS+ hosts configure with the [tacacs-server host](#) command.

server-group - Specifies the name of a server group configured with the [aaa group server](#) command. (Range: 1-64 characters)

Default Setting

Accounting is not enabled

No servers are specified

Command Mode

Global Configuration

Command Usage

Note that the **default** and *method-name* fields are only used to describe the accounting method(s) configured on the specified RADIUS or TACACS+ servers, and do not actually send any information to the servers about the methods to use.

Example

```
Console(config)#aaa accounting dot1x default start-stop group radius
Console(config)#
```

aaa accounting exec This command enables the accounting of requested Exec services for network access. Use the **no** form to disable the accounting service.

Syntax

aaa accounting exec {**default** | *method-name*}
start-stop group {**radius** | **tacacs+** | *server-group*}

no aaa accounting exec {**default** | *method-name*}

default - Specifies the default accounting method for service requests.

method-name - Specifies an accounting method for service requests.
 (Range: 1-64 characters)

start-stop - Records accounting from starting point and stopping point.

group - Specifies the server group to use.

radius - Specifies all RADIUS hosts configure with the [radius-server host](#) command.

tacacs+ - Specifies all TACACS+ hosts configure with the [tacacs-server host](#) command.

server-group - Specifies the name of a server group configured with the [aaa group server](#) command. (Range: 1-64 characters)

Default Setting

Accounting is not enabled
No servers are specified

Command Mode

Global Configuration

Command Usage

- ◆ This command runs accounting for Exec service requests for the local console and Telnet connections.
- ◆ Note that the **default** and *method-name* fields are only used to describe the accounting method(s) configured on the specified RADIUS or TACACS+ servers, and do not actually send any information to the servers about the methods to use.

Example

```
Console(config)#aaa accounting exec default start-stop group tacacs+
Console(config)#
```

aaa accounting update This command enables the sending of periodic updates to the accounting server. Use the **no** form to disable accounting updates.

Syntax

aaa accounting update [*periodic interval*]

no aaa accounting update

interval - Sends an interim accounting record to the server at this interval.
(Range: 1-2147483647 minutes)

Default Setting

1 minute

Command Mode

Global Configuration

Command Usage

- ◆ When accounting updates are enabled, the switch issues periodic interim accounting records for all users on the system.
- ◆ Using the command without specifying an interim interval enables updates, but does not change the current interval setting.

Example

```
Console(config)#aaa accounting update periodic 30
Console(config)#
```

aaa authorization exec This command enables the authorization for Exec access. Use the **no** form to disable the authorization service.

Syntax

aaa authorization exec {**default** | *method-name*}
group {**tacacs+** | *server-group*}

no aaa authorization exec {**default** | *method-name*}

default - Specifies the default authorization method for Exec access.

method-name - Specifies an authorization method for Exec access.
(Range: 1-64 characters)

group - Specifies the server group to use.

tacacs+ - Specifies all TACACS+ hosts configured with the [tacacs-server host](#) command.

server-group - Specifies the name of a server group configured with the [aaa group server](#) command. (Range: 1-64 characters)

Default Setting

Authorization is not enabled

No servers are specified

Command Mode

Global Configuration

Command Usage

- ◆ This command performs authorization to determine if a user is allowed to run an Exec shell.
- ◆ AAA authentication must be enabled before authorization is enabled.
- ◆ If this command is issued without a specified named method, the default method list is applied to all interfaces or lines (where this authorization type applies), except those that have a named method explicitly defined.

Example

```
Console(config)#aaa authorization exec default group tacacs+
Console(config)#
```

aaa group server Use this command to name a group of security server hosts. To remove a server group from the configuration list, enter the **no** form of this command.

Syntax

[no] aaa group server {radius | tacacs+} group-name

radius - Defines a RADIUS server group.

tacacs+ - Defines a TACACS+ server group.

group-name - A text string that names a security server group.
(Range: 1-64 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#aaa group server radius tps
Console(config-sg-radius)#
```

server This command adds a security server to an AAA server group. Use the **no** form to remove the associated server from the group.

Syntax

[no] server {index | ip-address}

index - Specifies the server index. (Range: RADIUS 1-5, TACACS+ 1)

ip-address - Specifies the host IP address of a server.

Default Setting

None

Command Mode

Server Group Configuration

Command Usage

- ◆ When specifying the index for a RADIUS server, that server index must already be defined by the [radius-server host](#) command.
- ◆ When specifying the index for a TACACS+ server, that server index must already be defined by the [tacacs-server host](#) command.

Example

```
Console(config)#aaa group server radius tps
Console(config-sg-radius)#server 10.2.68.120
Console(config-sg-radius)#
```

accounting dot1x This command applies an accounting method for 802.1X service requests on an interface. Use the **no** form to disable accounting on the interface.

Syntax

accounting dot1x {**default** | *list-name*}

no accounting dot1x

default - Specifies the default method list created with the [aaa accounting dot1x](#) command.

list-name - Specifies a method list created with the [aaa accounting dot1x](#) command.

Default Setting

None

Command Mode

Interface Configuration

Example

```
Console(config)#interface ethernet 1/2
Console(config-if)#accounting dot1x tps
Console(config-if)#
```

accounting exec This command applies an accounting method to local console, Telnet or SSH connections. Use the **no** form to disable accounting on the line.

Syntax

accounting exec {**default** | *list-name*}

no accounting exec

default - Specifies the default method list created with the [aaa accounting exec](#) command.

list-name - Specifies a method list created with the [aaa accounting exec](#) command.

Default Setting

None

Command Mode

Line Configuration

Example

```

Console(config)#line console
Console(config-line)#accounting exec tps
Console(config-line)#exit
Console(config)#line vty
Console(config-line)#accounting exec default
Console(config-line)#

```

authorization exec This command applies an authorization method to local console, Telnet or SSH connections. Use the **no** form to disable authorization on the line.

Syntax

authorization exec {default | *list-name*}
no authorization exec

default - Specifies the default method list created with the [aaa authorization exec](#) command.

list-name - Specifies a method list created with the [aaa authorization exec](#) command.

Default Setting

None

Command Mode

Line Configuration

Example

```

Console(config)#line console
Console(config-line)#authorization exec tps
Console(config-line)#exit
Console(config)#line vty
Console(config-line)#authorization exec default
Console(config-line)#

```

show accounting This command displays the current accounting settings per function and per port.

Syntax

show accounting
 [[**dot1x** [**statistics** [**username** *user-name* | **interface** *interface*]] |
exec [**statistics**] | **statistics**]

dot1x - Displays dot1x accounting information.

exec - Displays Exec accounting records.

statistics - Displays accounting records.

user-name - Displays accounting records for a specifiable username.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show accounting
Accounting Type : dot1x
  Method List   : default
  Group List    : radius
  Interface     : Eth 1/1

  Method List   : tps
  Group List    : radius
  Interface     : Eth 1/2

Accounting Type: EXEC
  Method List   : default
  Group List    : tacacs+
  Interface     : vty

Console#
```

Web Server

This section describes commands used to configure web browser management access to the switch.

Table 42: Web Server Commands

Command	Function	Mode
<code>ip http port</code>	Specifies the port to be used by the web browser interface	GC
<code>ip http server</code>	Allows the switch to be monitored or configured from a browser	GC
<code>ip http secure-port</code>	Specifies the UDP port number for HTTPS	GC
<code>ip http secure-server</code>	Enables HTTPS (HTTP/SSL) for encrypted communications	GC



Note: Users are automatically logged off of the HTTP server or HTTPS server if no input is detected for 300 seconds.

ip http port This command specifies the TCP port number used by the web browser interface. Use the **no** form to use the default port.

Syntax

ip http port *port-number*

no ip http port

port-number - The TCP port to be used by the browser interface.
(Range: 1-65535)

Default Setting

80

Command Mode

Global Configuration

Example

```
Console(config)#ip http port 769
Console(config)#
```

Related Commands

[ip http server \(238\)](#)

[show system \(116\)](#)

ip http server This command allows this device to be monitored or configured from a browser. Use the **no** form to disable this function.

Syntax

[no] ip http server

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#ip http server
Console(config)#
```

Related Commands

[ip http port \(238\)](#)

[show system \(116\)](#)

ip http secure-port This command specifies the UDP port number used for HTTPS connection to the switch's web interface. Use the **no** form to restore the default port.

Syntax

ip http secure-port *port_number*

no ip http secure-port

port_number – The UDP port used for HTTPS. (Range: 1-65535)

Default Setting

443

Command Mode

Global Configuration

Command Usage

- ◆ You cannot configure the HTTP and HTTPS servers to use the same port.
- ◆ If you change the HTTPS port number, clients attempting to connect to the HTTPS server must specify the port number in the URL, in this format: **https://device:port_number**

Example

```
Console(config)#ip http secure-port 1000
Console(config)#
```

Related Commands

[ip http secure-server \(239\)](#)

[show system \(116\)](#)

ip http secure-server This command enables the secure hypertext transfer protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (i.e., an encrypted connection) to the switch's web interface. Use the **no** form to disable this function.

Syntax

[no] ip http secure-server

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

- ◆ Both HTTP and HTTPS service can be enabled independently on the switch. However, you cannot configure the HTTP and HTTPS servers to use the same UDP port.
- ◆ If you enable HTTPS, you must indicate this in the URL that you specify in your browser: **https://device[:port_number]**
- ◆ When you start HTTPS, the connection is established in this way:
 - The client authenticates the server using the server's digital certificate.
 - The client and server negotiate a set of security protocols to use for the connection.
 - The client and server generate session keys for encrypting and decrypting data.
- ◆ The client and server establish a secure encrypted connection.
A padlock icon should appear in the status bar for Internet Explorer 6 or above, and Mozilla Firefox 17 or above.

The following web browsers and operating systems currently support HTTPS:

Table 43: HTTPS System Support

Web Browser	Operating System
Internet Explorer 6.x or later	Windows 98, Windows NT (with service pack 6a), Windows 2000, Windows XP, Windows Vista, Windows 7, Windows 8
Mozilla Firefox 17 or later	Windows 2000, Windows XP, Windows Vista, Windows 7, Windows 8, Linux

- ◆ To specify a secure-site certificate, see "Replacing the Default Secure-site Certificate" in the *Web Management Guide*. Also refer to the [copy tftp https-certificate](#) command.
- ◆ Connection to the web interface is not supported for HTTPS using an IPv6 link local address.

Example

```
Console(config)#ip http secure-server
Console(config)#
```

Related Commands

[ip http secure-port \(239\)](#)
[copy tftp https-certificate \(125\)](#)
[show system \(116\)](#)

Telnet Server

This section describes commands used to configure Telnet management access to the switch.

Table 44: Telnet Server Commands

Command	Function	Mode
<code>ip telnet max-sessions</code>	Specifies the maximum number of Telnet sessions that can simultaneously connect to this system	GC
<code>ip telnet port</code>	Specifies the port to be used by the Telnet interface	GC
<code>ip telnet server</code>	Allows the switch to be monitored or configured from Telnet	GC
<code>show ip telnet</code>	Displays configuration settings for the Telnet server	PE



Note: This switch also supports a Telnet client function. A Telnet connection can be made from this switch to another device by entering the **telnet** command at the Privileged Exec configuration level.

ip telnet max-sessions This command specifies the maximum number of Telnet sessions that can simultaneously connect to this system. Use the **no** from to restore the default setting.

Syntax

ip telnet max-sessions *session-count*

no ip telnet max-sessions

session-count - The maximum number of allowed Telnet session.
(Range: 0-8)

Default Setting

8 sessions

Command Mode

Global Configuration

Command Usage

A maximum of eight sessions can be concurrently opened for Telnet and Secure Shell (i.e., both Telnet and SSH share a maximum number or eight sessions).

Example

```
Console(config)#ip telnet max-sessions 1
Console(config)#
```

ip telnet port This command specifies the TCP port number used by the Telnet interface. Use the **no** form to use the default port.

Syntax

ip telnet port *port-number*

no telnet port

port-number - The TCP port number to be used by the browser interface.
(Range: 1-65535)

Default Setting

23

Command Mode

Global Configuration

Example

```
Console(config)#ip telnet port 123
Console(config)#
```

ip telnet server This command allows this device to be monitored or configured from Telnet. Use the **no** form to disable this function.

Syntax

[no] ip telnet server

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#ip telnet server
Console(config)#
```

show ip telnet This command displays the configuration settings for the Telnet server.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show ip telnet
IP Telnet Configuration:

Telnet Status: Enabled
Telnet Service Port: 23
Telnet Max Session: 4
Console#
```

Secure Shell

This section describes the commands used to configure the SSH server. Note that you also need to install a SSH client on the management station when using this protocol to configure the switch.



Note: The switch supports both SSH Version 1.5 and 2.0 clients.

Table 45: Secure Shell Commands

Command	Function	Mode
<code>ip ssh authentication-retries</code>	Specifies the number of retries allowed by a client	GC
<code>ip ssh server</code>	Enables the SSH server on the switch	GC
<code>ip ssh server-key size</code>	Sets the SSH server key size	GC
<code>ip ssh timeout</code>	Specifies the authentication timeout for the SSH server	GC
<code>copy tftp public-key</code>	Copies the user's public key from a TFTP server to the switch	PE
<code>delete public-key</code>	Deletes the public key for the specified user	PE
<code>disconnect</code>	Terminates a line connection	PE
<code>ip ssh crypto host-key generate</code>	Generates the host key	PE
<code>ip ssh crypto zeroize</code>	Clear the host key from RAM	PE
<code>ip ssh save host-key</code>	Saves the host key from RAM to flash memory	PE
<code>show ip ssh</code>	Displays the status of the SSH server and the configured values for authentication timeout and retries	PE
<code>show public-key</code>	Shows the public key for the specified user or for the host	PE

Table 45: Secure Shell Commands (Continued)

Command	Function	Mode
<code>show ssh</code>	Displays the status of current SSH sessions	PE
<code>show users</code>	Shows SSH users, including privilege level and public key type	PE

Configuration Guidelines

The SSH server on this switch supports both password and public key authentication. If password authentication is specified by the SSH client, then the password can be authenticated either locally or via a RADIUS or TACACS+ remote authentication server, as specified by the `authentication login` command. If public key authentication is specified by the client, then you must configure authentication keys on both the client and the switch as described in the following section. Note that regardless of whether you use public key or password authentication, you still have to generate authentication keys on the switch and enable the SSH server.

To use the SSH server, complete these steps:

1. Generate a Host Key Pair – Use the `ip ssh crypto host-key generate` command to create a host public/private key pair.
2. Provide Host Public Key to Clients – Many SSH client programs automatically import the host public key during the initial connection setup with the switch. Otherwise, you need to manually create a known hosts file on the management station and place the host public key in it. An entry for a public key in the known hosts file would appear similar to the following example:

```
10.1.0.54 1024 35 15684995401867669259333946775054617325313674890836547254
15020245593199868544358361651999923329781766065830956
108259132128902337654680172627257141342876294130119619556678259566410486957427
888146206519417467729848654686157177393901647793559423035774130980227370877945
4524083971752646358058176716709574804776117
```

3. Import Client's Public Key to the Switch – Use the `copy tftp public-key` command to copy a file containing the public key for all the SSH client's granted management access to the switch. (Note that these clients must be configured locally on the switch with the `username` command.) The clients are subsequently authenticated using these keys. The current firmware only accepts public key files based on standard UNIX format as shown in the following example for an RSA key:

```
1024 35
134108168560989392104094492015542534763164192187295892114317388005553616163105
177594083868631109291232226828519254374603100937187721199696317813662774141689
851320491172048303392543241016379975923714490119380060902539484084827178194372
288402533115952134861022902978982721353267131629432532818915045306393916643
steve@192.168.1.19
```

4. Set the Optional Parameters – Set other optional parameters, including the authentication timeout, the number of retries, and the server key size.
5. Enable SSH Service – Use the `ip ssh server` command to enable the SSH server on the switch.
6. *Authentication* – One of the following authentication methods is employed:

Password Authentication (for SSH v1.5 or V2 Clients)

- a. The client sends its password to the server.
- b. The switch compares the client's password to those stored in memory.
- c. If a match is found, the connection is allowed.



Note: To use SSH with only password authentication, the host public key must still be given to the client, either during initial connection or manually entered into the known host file. However, you do not need to configure the client's keys.

Public Key Authentication – When an SSH client attempts to contact the switch, the SSH server uses the host key pair to negotiate a session key and encryption method. Only clients that have a private key corresponding to the public keys stored on the switch can access it. The following exchanges take place during this process:

Authenticating SSH v1.5 Clients

- a. The client sends its RSA public key to the switch.
- b. The switch compares the client's public key to those stored in memory.
- c. If a match is found, the switch uses its secret key to generate a random 256-bit string as a challenge, encrypts this string with the user's public key, and sends it to the client.
- d. The client uses its private key to decrypt the challenge string, computes the MD5 checksum, and sends the checksum back to the switch.
- e. The switch compares the checksum sent from the client against that computed for the original string it sent. If the two check sums match, this means that the client's private key corresponds to an authorized public key, and the client is authenticated.

Authenticating SSH v2 Clients

- a. The client first queries the switch to determine if DSA public key authentication using a preferred algorithm is acceptable.
- b. If the specified algorithm is supported by the switch, it notifies the client to proceed with the authentication process. Otherwise, it rejects the request.
- c. The client sends a signature generated using the private key to the switch.

- d. When the server receives this message, it checks whether the supplied key is acceptable for authentication, and if so, it then checks whether the signature is correct. If both checks succeed, the client is authenticated.



Note: The SSH server supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.

Note: The SSH server can be accessed using any configured IPv4 or IPv6 interface address on the switch.

ip ssh authentication-retries This command configures the number of times the SSH server attempts to reauthenticate a user. Use the **no** form to restore the default setting.

Syntax

ip ssh authentication-retries *count*

no ip ssh authentication-retries

count – The number of authentication attempts permitted after which the interface is reset. (Range: 1-5)

Default Setting

3

Command Mode

Global Configuration

Example

```
Console(config)#ip ssh authentication-retries 2
Console(config)#
```

Related Commands

[show ip ssh \(251\)](#)

ip ssh server This command enables the Secure Shell (SSH) server on this switch. Use the **no** form to disable this service.

Syntax

[no] ip ssh server

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ The SSH server supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.
- ◆ The SSH server uses DSA or RSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.
- ◆ You must generate DSA and RSA host keys before enabling the SSH server.

Example

```
Console#ip ssh crypto host-key generate dsa
Console#configure
Console(config)#ip ssh server
Console(config)#
```

Related Commands

[ip ssh crypto host-key generate \(249\)](#)

[show ssh \(252\)](#)

ip ssh server-key size This command sets the SSH server key size. Use the **no** form to restore the default setting.

Syntax

ip ssh server-key size *key-size*

no ip ssh server-key size

key-size – The size of server key. (Range: 512-896 bits)

Default Setting

768 bits

Command Mode

Global Configuration

Command Usage

The server key is a private key that is never shared outside the switch. The host key is shared with the SSH client, and is fixed at 1024 bits.

Example

```
Console(config)#ip ssh server-key size 512
Console(config)#
```

ip ssh timeout This command configures the timeout for the SSH server. Use the **no** form to restore the default setting.

Syntax

ip ssh timeout *seconds*

no ip ssh timeout

seconds – The timeout for client response during SSH negotiation.
(Range: 1-120)

Default Setting

10 seconds

Command Mode

Global Configuration

Command Usage

The **timeout** specifies the interval the switch will wait for a response from the client during the SSH negotiation phase. Once an SSH session has been established, the timeout for user input is controlled by the [exec-timeout](#) command for vty sessions.

Example

```
Console(config)#ip ssh timeout 60
Console(config)#
```

Related Commands

[exec-timeout \(136\)](#)

[show ip ssh \(251\)](#)

delete public-key This command deletes the specified user's public key.

Syntax

delete public-key *username* [**dsa** | **rsa**]

username – Name of an SSH user. (Range: 1-8 characters)

dsa – DSA public key type.

rsa – RSA public key type.

Default Setting

Deletes both the DSA and RSA key.

Command Mode

Privileged Exec

Example

```
Console#delete public-key admin dsa
Console#
```

ip ssh crypto host-key generate This command generates the host key pair (i.e., public and private).

Syntax

ip ssh crypto host-key generate [dsa | rsa]

dsa – DSA (Version 2) key type.

rsa – RSA (Version 1) key type.

Default Setting

Generates both the DSA and RSA key pairs.

Command Mode

Privileged Exec

Command Usage

- ◆ The switch uses only RSA Version 1 for SSHv1.5 clients and DSA Version 2 for SSHv2 clients.
- ◆ This command stores the host key pair in memory (i.e., RAM). Use the [ip ssh save host-key](#) command to save the host key pair to flash memory.
- ◆ Some SSH client programs automatically add the public key to the known hosts file as part of the configuration process. Otherwise, you must manually create a known hosts file and place the host public key in it.
- ◆ The SSH server uses this host key to negotiate a session key and encryption method with the client trying to connect to it.

Example

```
Console#ip ssh crypto host-key generate dsa
Console#
```

Related Commands

[ip ssh crypto zeroize \(250\)](#)

[ip ssh save host-key \(250\)](#)

ip ssh crypto zeroize This command clears the host key from memory (i.e. RAM).

Syntax

ip ssh crypto zeroize [**dsa** | **rsa**]

dsa – DSA key type.

rsa – RSA key type.

Default Setting

Clears both the DSA and RSA key.

Command Mode

Privileged Exec

Command Usage

- ◆ This command clears the host key from volatile memory (RAM). Use the **no ip ssh save host-key** command to clear the host key from flash memory.
- ◆ The SSH server must be disabled before you can execute this command.

Example

```
Console#ip ssh crypto zeroize dsa
Console#
```

Related Commands

[ip ssh crypto host-key generate \(249\)](#)

[ip ssh save host-key \(250\)](#)

[no ip ssh server \(246\)](#)

ip ssh save host-key This command saves the host key from RAM to flash memory.

Syntax

ip ssh save host-key

Default Setting

Saves both the DSA and RSA key.

Command Mode

Privileged Exec

Example

```
Console#ip ssh save host-key dsa
Console#
```

Related Commands

[ip ssh crypto host-key generate \(249\)](#)

show ip ssh This command displays the connection settings used when authenticating client access to the SSH server.

Command Mode

Privileged Exec

Example

```
Console#show ip ssh
SSH Enabled - Version 2.0
Negotiation Timeout : 120 seconds; Authentication Retries : 3
Server Key Size      : 768 bits
Console#
```

show public-key This command shows the public key for the specified user or for the host.

Syntax

show public-key [user [username]] host]

username – Name of an SSH user. (Range: 1-8 characters)

Default Setting

Shows all public keys.

Command Mode

Privileged Exec

Command Usage

- ◆ If no parameters are entered, all keys are displayed. If the user keyword is entered, but no user name is specified, then the public keys for all users are displayed.
- ◆ When an RSA key is displayed, the first field indicates the size of the host key (e.g., 1024), the second field is the encoded public exponent (e.g., 35), and the last string is the encoded modulus. When a DSA key is displayed, the first field indicates that the encryption method used by SSH is based on the Digital Signature Standard (DSS), and the last string is the encoded modulus.

Example

```
Console#show public-key host
Host:
RSA:
1024 65537 13236940658254764031382795526536375927835525327972629521130241
071942106165575942459093923609695405036277525755625100386613098939383452310
332802149888661921595568598879891919505883940181387440468908779160305837768
```

```
185490002831341625008348718449522087429212255691665655296328163516964040831
5547660664151657116381
DSA:
ssh-dss AAAB3NzaC1kc3MAAACBAPWKZTPbsRIB8ydEXcxM3dyV/yrDbKStIlnzD/Dg0h2Hxc
YV44sXZ2JXhamLK6P8bvuiyacWbUW/a4PAtp1KMSdqsKeh3hKoA3vRRSy1N2XFfAKx15fwFfv
JlPdOkFgzLGMinvSNYQwiQXbKTBH0Z4mUZpE85PWxDZMacNBpjBrRAAAAFQChb4vsdfQGNIjwbv
wrNLaQ77isiwAAAIEasy5YWDC99ebYHNRj5kh47wY4i8cZvH+/p9cnrfwFTMU01VFDly3IR
2G395NLy5Qd7ZDxfA9mCOFT/yyEfbbobMJZi8oGCstSN0xrZZVnMqWrTYfdrKX7YKBw/Kjw6Bm
iFq70+jAhf1Dg45loAc27s6TLdtnylwRq/ow2eTCD5nekAAACBAJ8rMccXTxHLFACzWS7EjOy
DbsloBfPuSAb4oAsyjKXKVYNLQkTLZfcFRu41bS2KV5LAwecsigF/+DjKGWtPNIQqabKgYCw2
o/dVzX4Gg+yqdTlYmGA7fHGm8ARGeiG4ssFKy4Z6DmYPXFum1Yg0fhLwuHpOSKdxT3kk475S7
w0W
Console#
```

show ssh This command displays the current SSH server connections.

Command Mode

Privileged Exec

Example

```
Console#show ssh
Connection Version State Username Encryption
0 2.0 Session-Started admin ctos aes128-cbc-hmac-md5
stoc aes128-cbc-hmac-md5
Console#
```

Table 46: show ssh - display description

Field	Description
Session	The session number. (Range: 0-3)
Version	The Secure Shell version number.
State	The authentication negotiation state. (Values: Negotiation-Started, Authentication-Started, Session-Started)
Username	The user name of the client.

802.1X Port Authentication

The switch supports IEEE 802.1X (dot1x) port-based access control that prevents unauthorized access to the network by requiring users to first submit credentials for authentication. Client authentication is controlled centrally by a RADIUS server using EAP (Extensible Authentication Protocol).

Table 47: 802.1X Port Authentication Commands

Command	Function	Mode
<i>General Commands</i>		
<code>dot1x default</code>	Resets all dot1x parameters to their default values	GC
<code>dot1x eapol-pass-through</code>	Passes EAPOL frames to all ports in STP forwarding state when dot1x is globally disabled	GC
<code>dot1x system-auth-control</code>	Enables dot1x globally on the switch.	GC
<i>Authenticator Commands</i>		
<code>dot1x intrusion-action</code>	Sets the port response to intrusion when authentication fails	IC
<code>dot1x max-reauth-req</code>	Sets the maximum number of times that the switch sends an EAP-request/identity frame to the client before restarting the authentication process	IC
<code>dot1x max-req</code>	Sets the maximum number of times that the switch retransmits an EAP request/identity packet to the client before it times out the authentication session	IC
<code>dot1x operation-mode</code>	Allows single or multiple hosts on an dot1x port	IC
<code>dot1x port-control</code>	Sets dot1x mode for a port interface	IC
<code>dot1x re-authentication</code>	Enables re-authentication for all ports	IC
<code>dot1x timeout quiet-period</code>	Sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client	IC
<code>dot1x timeout re-authperiod</code>	Sets the time period after which a connected client must be re-authenticated	IC
<code>dot1x timeout supp-timeout</code>	Sets the interval for a supplicant to respond	IC
<code>dot1x timeout tx-period</code>	Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet	IC
<code>dot1x re-authenticate</code>	Forces re-authentication on specific ports	PE
<i>Display Information Commands</i>		
<code>show dot1x</code>	Shows all dot1x related information	PE

General Commands

dot1x default This command sets all configurable dot1x global and port settings to their default values.

Command Mode

Global Configuration

Example

```
Console(config)#dot1x default
Console(config)#
```

dot1x eapol-pass-through This command passes EAPOL frames through to all ports in STP forwarding state when dot1x is globally disabled. Use the **no** form to restore the default.

Syntax

[no] dot1x eapol-pass-through

Default Setting

Discards all EAPOL frames when dot1x is globally disabled

Command Mode

Global Configuration

Command Usage

- ◆ When this device is functioning as intermediate node in the network and does not need to perform dot1x authentication, the **dot1x eapol pass-through** command can be used to forward EAPOL frames from other switches on to the authentication servers, thereby allowing the authentication process to still be carried out by switches located on the edge of the network.
- ◆ When this device is functioning as an edge switch but does not require any attached clients to be authenticated, the **no dot1x eapol-pass-through** command can be used to discard unnecessary EAPOL traffic.

Example

This example instructs the switch to pass all EAPOL frame through to any ports in STP forwarding state.

```
Console(config)#dot1x eapol-pass-through
Console(config)#
```

dot1x system-auth-control This command enables IEEE 802.1X port authentication globally on the switch. Use the **no** form to restore the default.

Syntax

[no] dot1x system-auth-control

Default Setting

Disabled

Command Mode

Global Configuration

Example

```
Console(config)#dot1x system-auth-control
Console(config)#
```

Authenticator Commands

dot1x intrusion-action This command sets the port's response to a failed authentication, either to block all traffic, or to assign all traffic for the port to a guest VLAN. Use the **no** form to reset the default.

Syntax

dot1x intrusion-action {block-traffic | guest-vlan}

no dot1x intrusion-action

block-traffic - Blocks traffic on this port.

guest-vlan - Assigns the user to the Guest VLAN.

Default

block-traffic

Command Mode

Interface Configuration

Command Usage

For guest VLAN assignment to be successful, the VLAN must be configured and set as active (see the [vlan database](#) command) and assigned as the guest VLAN for the port (see the [network-access guest-vlan](#) command).

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x intrusion-action guest-vlan
Console(config-if)#
```

dot1x max-reauth-req This command sets the maximum number of times that the switch sends an EAP-request/identity frame to the client before restarting the authentication process. Use the **no** form to restore the default.

Syntax

dot1x max-reauth-req *count*

no dot1x max-reauth-req

count – The maximum number of requests (Range: 1-10)

Default

2

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x max-reauth-req 2
Console(config-if)#
```

dot1x max-req This command sets the maximum number of times the switch port will retransmit an EAP request/identity packet to the client before it times out the authentication session. Use the **no** form to restore the default.

Syntax

dot1x max-req *count*

no dot1x max-req

count – The maximum number of requests (Range: 1-10)

Default

2

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x max-req 2
Console(config-if)#
```


dot1x operation-mode This command allows hosts (clients) to connect to an 802.1X-authorized port. Use the **no** form with no keywords to restore the default to single host. Use the **no** form with the **multi-host max-count** keywords to restore the default maximum count.

Syntax

dot1x operation-mode {**single-host** | **multi-host** [**max-count** *count*] | **mac-based-auth**}

no dot1x operation-mode [**multi-host max-count**]

single-host – Allows only a single host to connect to this port.

multi-host – Allows multiple host to connect to this port.

max-count – Keyword for the maximum number of hosts.

count – The maximum number of hosts that can connect to a port.
(Range: 1-1024; Default: 5)

mac-based – Allows multiple hosts to connect to this port, with each host needing to be authenticated.

Default

Single-host

Command Mode

Interface Configuration

Command Usage

- ◆ The “max-count” parameter specified by this command is only effective if the dot1x mode is set to “auto” by the [dot1x port-control](#) command.
- ◆ In “multi-host” mode, only one host connected to a port needs to pass authentication for all other hosts to be granted network access. Similarly, a port can become unauthorized for all hosts if one attached host fails re-authentication or sends an EAPOL logoff message.
- ◆ In “mac-based-auth” mode, each host connected to a port needs to pass authentication. The number of hosts allowed access to a port operating in this mode is limited only by the available space in the secure address table (i.e., up to 1024 addresses).

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x operation-mode multi-host max-count 10
Console(config-if)#
```

dot1x port-control This command sets the dot1x mode on a port interface. Use the **no** form to restore the default.

Syntax

dot1x port-control {auto | force-authorized | force-unauthorized}

no dot1x port-control

auto – Requires a dot1x-aware connected client to be authorized by the RADIUS server. Clients that are not dot1x-aware will be denied access.

force-authorized – Configures the port to grant access to all clients, either dot1x-aware or otherwise.

force-unauthorized – Configures the port to deny access to all clients, either dot1x-aware or otherwise.

Default

force-authorized

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x port-control auto
Console(config-if)#
```

dot1x re-authentication This command enables periodic re-authentication for a specified port. Use the **no** form to disable re-authentication.

Syntax

[no] dot1x re-authentication

Command Mode

Interface Configuration

Command Usage

- ◆ The re-authentication process verifies the connected client's user ID and password on the RADIUS server. During re-authentication, the client remains connected the network and the process is handled transparently by the dot1x client software. Only if re-authentication fails is the port blocked.
- ◆ The connected client is re-authenticated after the interval specified by the **dot1x timeout re-authperiod** command. The default is 3600 seconds.

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x re-authentication
Console(config-if)#
```

Related Commands

[dot1x timeout re-authperiod \(259\)](#)

dot1x timeout quiet-period This command sets the time that a switch port waits after the maximum request count (see [page 256](#)) has been exceeded before attempting to acquire a new client. Use the **no** form to reset the default.

Syntax

dot1x timeout quiet-period *seconds*

no dot1x timeout quiet-period

seconds - The number of seconds. (Range: 1-65535)

Default

60 seconds

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout quiet-period 350
Console(config-if)#
```

dot1x timeout re-authperiod This command sets the time period after which a connected client must be re-authenticated. Use the **no** form of this command to reset the default.

Syntax

dot1x timeout re-authperiod *seconds*

no dot1x timeout re-authperiod

seconds - The number of seconds. (Range: 1-65535)

Default

3600 seconds

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout re-authperiod 300
Console(config-if)#
```

dot1x timeout supp-timeout This command sets the time that an interface on the switch waits for a response to an EAP request from a client before re-transmitting an EAP packet. Use the **no** form to reset to the default value.

Syntax

dot1x timeout supp-timeout *seconds*

no dot1x timeout supp-timeout

seconds - The number of seconds. (Range: 1-65535)

Default

30 seconds

Command Mode

Interface Configuration

Command Usage

This command sets the timeout for EAP-request frames other than EAP-request/identity frames. If dot1x authentication is enabled on a port, the switch will initiate authentication when the port link state comes up. It will send an EAP-request/identity frame to the client to request its identity, followed by one or more requests for authentication information. It may also send other EAP-request frames to the client during an active connection as required for reauthentication.

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout supp-timeout 300
Console(config-if)#
```

dot1x timeout tx-period This command sets the time that an interface on the switch waits during an authentication session before re-transmitting an EAP packet. Use the **no** form to reset to the default value.

Syntax

dot1x timeout tx-period *seconds*

no dot1x timeout tx-period

seconds - The number of seconds. (Range: 1-65535)

Default

30 seconds

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout tx-period 300
Console(config-if)#
```

dot1x re-authenticate This command forces re-authentication on all ports or a specific interface.

Syntax

dot1x re-authenticate [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

Command Mode

Privileged Exec

Command Usage

The re-authentication process verifies the connected client's user ID and password on the RADIUS server. During re-authentication, the client remains connected the network and the process is handled transparently by the dot1x client software. Only if re-authentication fails is the port blocked.

Example

```
Console#dot1x re-authenticate
Console#
```

Display Information Commands

show dot1x This command shows general port authentication related settings on the switch or a specific interface.

Syntax

show dot1x [**statistics**] [**interface** *interface*]

statistics - Displays dot1x status for each port.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

Command Mode

Privileged Exec

Command Usage

This command displays the following information:

- ◆ *Global 802.1X Parameters* – Shows whether or not 802.1X port authentication is globally enabled on the switch ([page 255](#)).
- ◆ *Authenticator Parameters* – Shows whether or not EAPOL pass-through is enabled ([page 254](#)).
- ◆ *802.1X Port Summary* – Displays the port access control parameters for each interface that has enabled 802.1X, including the following items:
 - Type – Administrative state for port access control (Enabled, Authenticator, or Supplicant).
 - Operation Mode–Allows single or multiple hosts ([page 257](#)).
 - Control Mode – Dot1x port control mode ([page 258](#)).
 - Authorized– Authorization status (yes or n/a - not authorized).
- ◆ *802.1X Port Details* – Displays the port access control parameters for each interface, including the following items:
 - Reauthentication – Periodic re-authentication ([page 258](#)).
 - Reauth Period – Time after which a connected client must be re-authenticated ([page 259](#)).
 - Quiet Period – Time a port waits after Max Request Count is exceeded before attempting to acquire a new client ([page 259](#)).
 - TX Period – Time a port waits during authentication session before re-transmitting EAP packet ([page 260](#)).
 - Supplicant Timeout – Supplicant timeout.
 - Server Timeout – Server timeout. A RADIUS server must be set before the correct operational value of 10 seconds will be displayed in this field.
 - Reauth Max Retries – Maximum number of reauthentication attempts.
 - Max Request – Maximum number of times a port will retransmit an EAP request/identity packet to the client before it times out the authentication session ([page 256](#)).
 - Operation Mode– Shows if single or multiple hosts (clients) can connect to an 802.1X-authorized port.
 - Port Control–Shows the dot1x mode on a port as auto, force-authorized, or force-unauthorized ([page 258](#)).
 - Intrusion Action– Shows the port response to intrusion when authentication fails ([page 255](#)).
 - Supplicant– MAC address of authorized client.

◆ *Authenticator PAE State Machine*

- State – Current state (including initialize, disconnected, connecting, authenticating, authenticated, aborting, held, force_authorized, force_unauthorized).
- Reauth Count– Number of times connecting state is re-entered.
- Current Identifier– The integer (0-255) used by the Authenticator to identify the current authentication session.

◆ *Backend State Machine*

- State – Current state (including request, response, success, fail, timeout, idle, initialize).
- Request Count– Number of EAP Request packets sent to the Supplicant without receiving a response.
- Identifier (Server)– Identifier carried in the most recent EAP Success, Failure or Request packet received from the Authentication Server.

◆ *Reauthentication State Machine*

State – Current state (including initialize, reauthenticate).

Example

```

Console#show dot1x
Global 802.1X Parameters
  System Auth Control      : Enabled

Authenticator Parameters:
  EAPOL Pass Through      : Disabled

802.1X Port Summary

Port      Type      Operation Mode Control Mode    Authorized
-----
Eth 1/ 1 Disabled    Single-Host    Force-Authorized Yes
Eth 1/ 2 Disabled    Single-Host    Force-Authorized Yes
.
.
Eth 1/51 Disabled    Single-Host    Force-Authorized Yes
Eth 1/52 Enabled     Single-Host    Auto           Yes

802.1X Port Details

802.1X Authenticator is enabled on port 1/1
802.1X Supplicant is disabled on port 1/1
.
.
802.1X Authenticator is enabled on port 28
Reauthentication      : Enabled
Reauth Period         : 3600
Quiet Period          : 60
TX Period              : 30
Supplicant Timeout    : 30
Server Timeout        : 10
Reauth Max Retries    : 2
Max Request           : 2
Operation Mode        : Multi-host
Port Control          : Auto
Intrusion Action      : Block traffic
  
```

```
Supplicant                : 00-e0-29-94-34-65
```

```
Authenticator PAE State Machine  
State                    : Authenticated  
Reauth Count             : 0  
Current Identifier       : 3
```

```
Backend State Machine  
State                    : Idle  
Request Count            : 0  
Identifier(Server)       : 2
```

```
Reauthentication State Machine  
State                    : Initialize
```

```
Console#
```

Management IP Filter

This section describes commands used to configure IP management access to the switch.

Table 48: Management IP Filter Commands

Command	Function	Mode
<code>management</code>	Configures IP addresses that are allowed management access	GC
<code>show management</code>	Displays the switch to be monitored or configured from a browser	PE

management This command specifies the client IP addresses that are allowed management access to the switch through various protocols. Use the **no** form to restore the default setting.

Syntax

```
[no] management {all-client | http-client | snmp-client | telnet-client}  
start-address [end-address]
```

all-client - Adds IP address(es) to all groups.

http-client - Adds IP address(es) to the web group.

snmp-client - Adds IP address(es) to the SNMP group.

telnet-client - Adds IP address(es) to the Telnet group.

start-address - A single IP address, or the starting address of a range.

end-address - The end address of a range.

Default Setting

All addresses

Command Mode

Global Configuration

Command Usage

- ◆ If anyone tries to access a management interface on the switch from an invalid address, the switch will reject the connection, enter an event message in the system log, and send a trap message to the trap manager.
- ◆ IP address can be configured for SNMP, web, and Telnet access respectively. Each of these groups can include up to five different sets of addresses, either individual addresses or address ranges.
- ◆ When entering addresses for the same group (i.e., SNMP, web, or Telnet), the switch will not accept overlapping address ranges. When entering addresses for different groups, the switch will accept overlapping address ranges.
- ◆ You cannot delete an individual address from a specified range. You must delete the entire range, and re-enter the addresses.
- ◆ You can delete an address range just by specifying the start address, or by specifying both the start address and end address.

Example

This example restricts management access to the indicated addresses.

```
Console(config)#management all-client 192.168.1.19
Console(config)#management all-client 192.168.1.25 192.168.1.30
Console#
```

show management This command displays the client IP addresses that are allowed management access to the switch through various protocols.

Syntax

show management {all-client | http-client | snmp-client | telnet-client}

all-client - Displays IP addresses for all groups.

http-client - Displays IP addresses for the web group.

snmp-client - Displays IP addresses for the SNMP group.

telnet-client - Displays IP addresses for the Telnet group.

Command Mode

Privileged Exec

Example

```
Console#show management all-client
Management Ip Filter
  HTTP-Client:
    Start IP address      End IP address
    -----
  1. 192.168.1.19         192.168.1.19
  2. 192.168.1.25         192.168.1.30

  SNMP-Client:
    Start IP address      End IP address
    -----
  1. 192.168.1.19         192.168.1.19
  2. 192.168.1.25         192.168.1.30

  TELNET-Client:
    Start IP address      End IP address
    -----
  1. 192.168.1.19         192.168.1.19
  2. 192.168.1.25         192.168.1.30

Console#
```

PPPoE Intermediate Agent

This section describes commands used to configure the PPPoE Intermediate Agent (PPPoE IA) relay parameters required for passing authentication messages between a client and broadband remote access servers.

Table 49: PPPoE Intermediate Agent Commands

Command	Function	Mode
pppoe intermediate-agent	Enables the PPPoE IA globally on the switch	GC
pppoe intermediate-agent format-type	Sets the access node identifier and generic error message for the switch	GC
pppoe intermediate-agent port-enable	Enables the PPPoE IA on an interface	IC
pppoe intermediate-agent port-format-type	Sets the circuit-id or remote-id for an interface	IC
pppoe intermediate-agent trust	Sets the trust mode for an interface	IC
pppoe intermediate-agent vendor-tag strip	Enables the stripping of vendor tags from PPPoE Discovery packets sent from a PPPoE server	IC
clear pppoe intermediate-agent statistics	Clears PPPoE IA statistics	PE
show pppoe intermediate-agent info	Displays PPPoE IA configuration settings	PE
show pppoe intermediate-agent statistics	Displays PPPoE IA statistics	PE

pppoe intermediate-agent This command enables the PPPoE Intermediate Agent globally on the switch. Use the **no** form to disable this feature.

Syntax

[no] pppoe intermediate-agent

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ The switch inserts a tag identifying itself as a PPPoE Intermediate Agent residing between the attached client requesting network access and the ports connected to broadband remote access servers (BRAS). The switch extracts access-loop information from the client's PPPoE Active Discovery Request, and forwards this information to all trusted ports designated by the **pppoe intermediate-agent trust** command. The BRAS detects the presence of the subscriber's circuit-Id tag inserted by the switch during the PPPoE discovery phase, and sends this tag as a NAS-port-Id attribute in PPP authentication and AAA accounting requests to a RADIUS server.
- ◆ PPPoE IA must be enabled globally by this command before this feature can be enabled on an interface using the **pppoe intermediate-agent port-enable** command.

Example

```
Console(config)#pppoe intermediate-agent
Console(config)#
```

pppoe intermediate-agent format-type This command sets the access node identifier and generic error message for the switch. Use the **no** form to restore the default settings.

Syntax

pppoe intermediate-agent format-type {access-node-identifier *id-string* | generic-error-message *error-message*}

no pppoe intermediate-agent format-type {access-node-identifier | generic-error-message}

id-string - String identifying this switch as an PPPoE IA to the PPPoE server.
(Range: 1-48 ASCII characters)

error-message - An error message notifying the sender that the PPPoE Discovery packet was too large.

Default Setting

- ◆ Access Node Identifier: IP address of the management interface
- ◆ Generic Error Message: PPPoE Discover packet too large to process. Try reducing the number of tags added.

Command Mode

Global Configuration

Command Usage

- ◆ The switch uses the access-node-identifier to generate the circuit-id for PPPoE discovery stage packets sent to the BRAS, but does not modify the source or destination MAC address of these PPPoE discovery packets.
- ◆ These messages are forwarded to all trusted ports designated by the `pppoe intermediate-agent trust` command.

Example

```
Console(config)#pppoe intermediate-agent format-type access-node-identifier  
billibong  
Console(config)#
```

pppoe intermediate-agent port-enable

This command enables the PPPoE IA on an interface. Use the **no** form to disable this feature.

Syntax

[no] pppoe intermediate-agent port-enable

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

PPPoE IA must also be enabled globally on the switch for this command to take effect.

Example

```
Console(config)#int ethernet 1/5  
Console(config-if)#pppoe intermediate-agent port-enable  
Console(config-if)#
```

pppoe intermediate-agent port-format-type

This command sets the circuit-id or remote-id for an interface. Use the **no** form to restore the default settings.

Syntax

pppoe intermediate-agent port-format-type {circuit-id | remote-id} id-string

circuit-id - String identifying the circuit identifier (or interface) on this switch to which the user is connected. (Range: 1-10 ASCII characters)

remote-id - String identifying the remote identifier (or interface) on this switch to which the user is connected. (Range: 1-63 ASCII characters)

Default Setting

circuit-id: unit/port:vlan-id or 0/trunk-id:vlan-id
remote-id: port MAC address

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ The PPPoE server extracts the Line-Id tag from PPPoE discovery stage messages, and uses the Circuit-Id field of that tag as a NAS-Port-Id attribute in AAA access and accounting requests.
- ◆ The switch intercepts PPPoE discovery frames from the client and inserts a unique line identifier using the PPPoE Vendor-Specific tag (0x0105) to PPPoE Active Discovery Initiation (PADI) and Request (PADR) packets. The switch then forwards these packets to the PPPoE server. The tag contains the Line-Id of the customer line over which the discovery packet was received, entering the switch (or access node) where the intermediate agent resides.
- ◆ Outgoing PAD Offer (PADO) and Session-confirmation (PADS) packets sent from the PPPoE Server include the Circuit-Id tag inserted by the switch, and should be stripped out of PADO and PADS packets which are to be passed directly to end-node clients using the [pppoe intermediate-agent vendor-tag strip](#) command.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#pppoe intermediate-agent port-format-type circuit-id
ECS4660-28F
Console(config-if)#
```

pppoe intermediate-agent trust This command sets an interface to trusted mode to indicate that it is connected to a PPPoE server. Use the **no** form to set an interface to untrusted mode.

Syntax

[no] pppoe intermediate-agent trust

Default Setting

Untrusted

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ Set any interfaces connecting the switch to a PPPoE Server as trusted. Interfaces that connect the switch to users (PPPoE clients) should be set as untrusted.
- ◆ At least one trusted interface must be configured on the switch for the PPPoE IA to function.

Example

```
Console(config)#int ethernet 1/5
Console(config-if)#pppoe intermediate-agent trust
Console(config-if)#
```

pppoe intermediate-agent vendor-tag strip This command enables the stripping of vendor tags from PPPoE Discovery packets sent from a PPPoE server. Use the **no** form to disable this feature.

Syntax

[no] pppoe intermediate-agent vendor-tag strip

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This command only applies to trusted interfaces. It is used to strip off vendor-specific tags (which carry subscriber and line identification information) in PPPoE Discovery packets received from an upstream PPPoE server before forwarding them to a user.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#pppoe intermediate-agent vendor-tag strip
Console(config-if)#
```

clear pppoe intermediate-agent statistics This command clears statistical counters for the PPPoE Intermediate Agent.

Syntax

clear pppoe intermediate-agent statistics interface [*interface*]
interface
ethernet *unit/port*
unit - Stack unit. (Range: 1)
port - Port number. (Range: 1-52)
port-channel *channel-id* (Range: 1-8)

Command Mode

Privileged Exec

Example

```
Console#clear pppoe intermediate-agent statistics
Console#
```

show pppoe intermediate-agent info This command displays configuration settings for the PPPoE Intermediate Agent.

Syntax

show pppoe intermediate-agent info [**interface** *interface*]
interface
ethernet *unit/port*
unit - Stack unit. (Range: 1)
port - Port number. (Range: 1-52)
port-channel *channel-id* (Range: 1-8)

Command Mode

Privileged Exec

Example

```
Console#show pppoe intermediate-agent info
PPPoE Intermediate Agent Global Status      : Enabled
PPPoE Intermediate Agent Admin Access Node Identifier : 192.168.0.2
PPPoE Intermediate Agent Oper Access Node Identifier  : 192.168.0.2
```

```

PPPoE Intermediate Agent Admin Generic Error Message :
PPPoE Discover packet too large to process. Try reducing the number of tags
added.
PPPoE Intermediate Agent Oper Generic Error Message :
PPPoE Discover packet too large to process. Try reducing the number of tags
added.
Console# show pppoe intermediate-agent info interface ethernet 1/1
Interface PPPoE IA Trusted Vendor-Tag Strip Admin Circuit-ID Admin Remote-ID
Oper Circuit-ID Oper Remote-ID
-----
Eth 1/2 Yes No Yes ECS5610-52S ECS5610-52S
ECS5610-52S ECS5610-52S
Console#

```

show pppoe intermediate-agent statistics This command displays statistics for the PPPoE Intermediate Agent.

Syntax

```

show pppoe intermediate-agent statistics interface [interface]
interface
    ethernet unit/port
        unit - Stack unit. (Range: 1)
        port - Port number. (Range: 1-52)
    port-channel channel-id (Range: 1-8)

```

Command Mode
Privileged Exec

Example

```

Console# show pppoe intermediate-agent statistics interface ethernet 1/1
Eth 1/1 statistics
-----
Received : All PADI PADO PADR PADS PADT
           3 0 0 0 0 3
Dropped : Response from untrusted Request towards untrusted Malformed
           0 0 0
Console#

```

Table 50: show pppoe intermediate-agent statistics - display description

Field	Description
<i>Received</i>	
PADI	PPPoE Active Discovery Initiation
PADO	PPPoE Active Discovery Offer
PADR	PPPoE Active Discovery Request

Table 50: show pppoe intermediate-agent statistics - display description

Field	Description
PADS	PPPoE Active Discovery Session-Confirmation
PADT	PPPoE Active Discovery Terminate
<i>Dropped</i>	
Response from untrusted	Response from an interface which not been configured as trusted.
Request towards untrusted	Request sent to an interface which not been configured as trusted.
Malformed	Corrupted PPPoE message.

General Security Measures

This switch supports many methods of segregating traffic for clients attached to each of the data ports, and for ensuring that only authorized clients gain access to the network. Port-based authentication using IEEE 802.1X is commonly used for these purposes. In addition to these method, several other options of providing client security are described in this chapter. These include port-based authentication, which can be configured to allow network client access by specifying a fixed set of MAC addresses. The addresses assigned to DHCP clients can also be carefully controlled with IP Source Guard and DHCP Snooping commands.

Table 51: General Security Commands

Command Group	Function
Port Security*	Configures secure addresses for a port
802.1X Port Authentication*	Configures host authentication on specific ports using 802.1X
Network Access*	Configures MAC authentication and dynamic VLAN assignment
Web Authentication*	Configures Web authentication
Access Control Lists*	Provides filtering for IP frames (based on address, protocol, TCP/UDP port number or TCP control code) or non-IP frames (based on MAC address or Ethernet type)
DHCPv4 Snooping*	Filters untrusted DHCP messages on unsecure ports by building and maintaining a DHCP snooping binding table
DHCPv6 Snooping*	Filters untrusted DHCPv6 messages on unsecure ports by building and maintaining a DHCPv6 snooping binding table
IPv4 Source Guard*	Filters IPv4 traffic on insecure ports for which the source address cannot be identified via DHCPv4 snooping nor static source bindings
IPv6 Source Guard*	Filters IPv6 traffic on insecure ports for which the source address cannot be identified via DHCPv6 snooping nor static source bindings
ARP Inspection	Validates the MAC-to-IP address bindings in ARP packets
DoS Protection	Protects against Denial-of-Service attacks
Port-based Traffic Segmentation	Configures traffic segmentation for different client sessions based on specified downlink and uplink ports

* The priority of execution for these filtering commands is Port Security, Port Authentication, Network Access, Web Authentication, Access Control Lists, DHCP Snooping, and then IP Source Guard.

Port Security

These commands can be used to enable port security on a port.

When MAC address learning is disabled on an interface, only incoming traffic with source addresses already stored in the dynamic or static address table for this port will be authorized to access the network.

When using port security, the switch stops learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table for this port will be authorized to access the network. The port will drop any incoming frames with a source MAC address that is unknown or has been previously learned from another port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.

Table 52: Management IP Filter Commands

Command	Function	Mode
<code>mac-address-table static</code>	Maps a static address to a port in a VLAN	GC
<code>mac-learning</code>	Enables MAC address learning on the selected physical interface or VLAN	IC
<code>port security</code>	Configures a secure port	IC
<code>show mac-address-table</code>	Displays entries in the bridge-forwarding database	PE
<code>show port security</code>	Displays port security status and secure address count	PE

mac-learning This command enables MAC address learning on the selected interface. Use the **no** form to disable MAC address learning.

Syntax

[no] mac-learning

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet or Port Channel)

Command Usage

- ◆ The **no mac-learning** command immediately stops the switch from learning new MAC addresses on the specified port or trunk. Only incoming traffic with source addresses stored in the static address table will be accepted. Note that the dynamic addresses stored in the address table when MAC address learning

is disabled are flushed from the system, and no dynamic addresses are subsequently learned until MAC address learning has been re-enabled.

- ◆ The mac-learning commands cannot be used if 802.1X Port Authentication has been globally enabled on the switch with the [dot1x system-auth-control](#) command, or if MAC Address Security has been enabled by the [port security](#) command on the same interface.

Example

The following example disables MAC address learning for port 2.

```
Console(config)#interface ethernet 1/2
Console(config-if)#no mac-learning
Console(config-if)#
```

Related Commands

[show interfaces status \(393\)](#)

port security This command enables or configures port security. Use the **no** form without any keywords to disable port security. Use the **no** form with the appropriate keyword to restore the default settings for a response to security violation or for the maximum number of allowed addresses.

Syntax

port security [**action** {**shutdown** | **trap** | **trap-and-shutdown**}
| **max-mac-count** *address-count*]

no port security [**action** | **max-mac-count**]

action - Response to take when port security is violated.

shutdown - Disable port only.

trap - Issue SNMP trap message only.

trap-and-shutdown - Issue SNMP trap message and disable port.

max-mac-count

address-count - The maximum number of MAC addresses that can be learned on a port. (Range: 0 - 1024, where 0 means disabled)

Default Setting

Status: Disabled

Action: None

Maximum Addresses: 0

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ The default maximum number of MAC addresses allowed on a secure port is zero (that is, port security is disabled). To use port security, you must configure the maximum number of addresses allowed on a port using the **port security max-mac-count** command.
- ◆ When port security is enabled using the **port security** command, or the maximum number or allowed addresses is set to value lower than the limit after port security has been enabled, the switch first clears all dynamically learned entries from the address table. It then starts learning new MAC addresses on the specified port, and stops learning addresses when it reaches a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted.
- ◆ To configure the maximum number of address entries which can be learned on a port, specify the maximum number of dynamic addresses allowed. The switch will learn up to the maximum number of allowed address pairs <source MAC address, VLAN> for frames received on the port. (The specified maximum address count is effective when port security is enabled or disabled.) Note that you can manually add additional secure addresses to a port using the [mac-address-table static](#) command. When the port has reached the maximum number of MAC addresses, the port will stop learning new addresses. The MAC addresses already in the address table will be retained and will not be aged out.
- ◆ If port security is enabled, and the maximum number of allowed addresses are set to a non-zero value, any device not in the address table that attempts to use the port will be prevented from accessing the switch.
- ◆ If a port is disabled due to a security violation, it must be manually re-enabled using the [no shutdown](#) command.
- ◆ A secure port has the following restrictions:
 - Cannot be connected to a network interconnection device.
 - Cannot be a trunk port.

Example

The following example enables port security for port 5, and sets the response to a security violation to issue a trap message:

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap
```

Related Commands

[show interfaces status](#) (393)

[shutdown](#) (376)

[mac-address-table static](#) (444)

show port security This command displays port security status and the secure address count.

Syntax

show port security [**interface** *interface*]

interface - Specifies a port interface.

ethernet *unit/port*

unit - This is unit 1.

port - Port number. (Range: 1-52)

Command Mode

Privileged Exec

Example

This example shows the port security settings and number of secure addresses for all ports.

```
Console#show port security
Global Port Security Parameters
Secure MAC Aging Mode : Disabled

Port Security Port Summary
Port      Port Security Port Status  Intrusion Action  MaxMacCnt  CurrMacCnt
-----
Eth 1/ 1 Disabled      Secure/Down  None           0           2
Eth 1/ 2 Enabled       Secure/Up    None          10           0
Eth 1/ 3 Disabled      Secure/Down  None           0           0
Eth 1/ 4 Disabled      Secure/Down  None           0           0
Eth 1/ 5 Disabled      Secure/Down  None           0           0
:
```

Table 53: show port security - display description

Field	Description
Port Security	The configured status (enabled or disabled).
Port Status	The operational status: <ul style="list-style-type: none"> ◆ Secure/Down – Port security is disabled. ◆ Secure/Up – Port security is enabled. ◆ Shutdown – Port is shut down due to a response to a port security violation.
Intrusion Action	The configured intrusion response.
MaxMacCnt	The maximum number of addresses which can be stored in the address table for this interface (either dynamic or static).
CurrMacCnt	The current number of secure entries in the address table.

The following example shows the port security settings and number of secure addresses for a specific port. The Last Intrusion MAC and Last Time Detected Intrusion MAC fields show information about the last detected intrusion MAC

address. These fields are not applicable if no intrusion has been detected or port security is disabled. The MAC Filter ID field is configured by the [network-access port-mac-filter](#) command. If this field displays Disabled, then any unknown source MAC address can be learned as a secure MAC address. If it displays a filter identifier, then only source MAC address entries in MAC Filter table can be learned as secure MAC addresses.

```
Console#show port security interface ethernet 1/2
Global Port Security Parameters
  Secure MAC aging mode : Disabled

Port Security Details
  Port : 1/2
  Port Security : Enabled
  Port Status : Secure/Up
  Intrusion Action : None
  Max-MAC-Count : 0
  Current MAC Count : 0
  MAC Filter ID : Disabled
  Last Intrusion MAC : NA
  Last Time Detected Intrusion MAC : NA
Console#
```

This example shows information about a detected intrusion.

```
Console#show port security interface ethernet 1/2
Global Port Security Parameters
  Secure MAC aging mode : Disabled

Port Security Details
  Port : 1/2
  Port Security : Enabled
  Port Status : Secure/Up
  Intrusion Action : None
  Max-MAC-Count : 0
  Current MAC Count : 0
  MAC Filter : Enabled
  MAC Filter ID : 1
  Last Intrusion MAC : 00-10-22-00-00-01
  Last Time Detected Intrusion MAC : 2010/7/29 15:13:03
Console#
```


Network Access (MAC Address Authentication)

Network Access authentication controls access to the network by authenticating the MAC address of each host that attempts to connect to a switch port. Traffic received from a specific MAC address is forwarded by the switch only if the source MAC address is successfully authenticated by a central RADIUS server. While authentication for a MAC address is in progress, all traffic is blocked until authentication is completed. Once successfully authenticated, the RADIUS server may optionally assign VLAN and QoS settings for the switch port.

Table 54: Network Access Commands

Command	Function	Mode
<code>network-access aging</code>	Enables MAC address aging	GC
<code>network-access mac-filter</code>	Adds a MAC address to a filter table	GC
<code>mac-authentication reauth-time</code>	Sets the time period after which a connected MAC address must be re-authenticated	GC
<code>network-access dynamic-qos</code>	Enables the dynamic quality of service feature	IC
<code>network-access dynamic-vlan</code>	Enables dynamic VLAN assignment from a RADIUS server	IC
<code>network-access guest-vlan</code>	Specifies the guest VLAN	IC
<code>network-access link-detection</code>	Enables the link detection feature	IC
<code>network-access link-detection link-down</code>	Configures the link detection feature to detect and act upon link-down events	IC
<code>network-access link-detection link-up</code>	Configures the link detection feature to detect and act upon link-up events	IC
<code>network-access link-detection link-up-down</code>	Configures the link detection feature to detect and act upon both link-up and link-down events	IC
<code>network-access max-mac-count</code>	Sets the maximum number of MAC addresses that can be authenticated on a port via all forms of authentication	IC
<code>network-access mode mac-authentication</code>	Enables MAC authentication on an interface	IC
<code>network-access port-mac-filter</code>	Enables the specified MAC address filter	IC
<code>mac-authentication intrusion-action</code>	Determines the port response when a connected host fails MAC authentication.	IC
<code>mac-authentication max-mac-count</code>	Sets the maximum number of MAC addresses that can be authenticated on a port via MAC authentication	IC
<code>clear network-access</code>	Clears authenticated MAC addresses from the address table	PE
<code>show network-access</code>	Displays the MAC authentication settings for port interfaces	PE
<code>show network-access mac-address-table</code>	Displays information for entries in the secure MAC address table	PE
<code>show network-access mac-filter</code>	Displays information for entries in the MAC filter tables	PE

network-access aging Use this command to enable aging for authenticated MAC addresses stored in the secure MAC address table. Use the **no** form of this command to disable address aging.

Syntax

[no] network-access aging

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ Authenticated MAC addresses are stored as dynamic entries in the switch's secure MAC address table and are removed when the aging time expires. The address aging time is determined by the [mac-address-table aging-time](#) command.
- ◆ This parameter applies to authenticated MAC addresses configured by the MAC Address Authentication process described in this section, as well as to any secure MAC addresses authenticated by 802.1X, regardless of the 802.1X Operation Mode (Single-Host, Multi-Host, or MAC-Based authentication as described on [page 257](#)).
- ◆ The maximum number of secure MAC addresses supported for the switch system is 1024.

Example

```
Console(config-if)#network-access aging
Console(config-if)#
```

network-access mac-filter Use this command to add a MAC address into a filter table. Use the **no** form of this command to remove the specified MAC address.

Syntax

**[no] network-access mac-filter *filter-id*
mac-address *mac-address* [*mask mask-address*]**

filter-id - Specifies a MAC address filter table. (Range: 1-64)

mac-address - Specifies a MAC address entry. (Format: xx-xx-xx-xx-xx-xx)

mask - Specifies a MAC address bit mask for a range of addresses.

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ Specified addresses are exempt from network access authentication.
- ◆ This command is different from configuring static addresses with the `mac-address-table static` command in that it allows you configure a range of addresses when using a mask, and then to assign these addresses to one or more ports with the `network-access port-mac-filter` command.
- ◆ Up to 64 filter tables can be defined.
- ◆ There is no limitation on the number of entries that can entered in a filter table.

Example

```
Console(config)#network-access mac-filter 1 mac-address 11-22-33-44-55-66  
Console(config)#
```

mac-authentication reauth-time

Use this command to set the time period after which a connected MAC address must be re-authenticated. Use the **no** form of this command to restore the default value.

Syntax

mac-authentication reauth-time *seconds*

no mac-authentication reauth-time

seconds - The reauthentication time period. (Range: 120-1000000 seconds)

Default Setting

1800

Command Mode

Global Configuration

Command Usage

- ◆ The reauthentication time is a global setting and applies to all ports.
- ◆ When the reauthentication time expires for a secure MAC address it is reauthenticated with the RADIUS server. During the reauthentication process traffic through the port remains unaffected.

Example

```
Console(config)#mac-authentication reauth-time 300  
Console(config)#
```

network-access dynamic-qos Use this command to enable the dynamic QoS feature for an authenticated port.
Use the **no** form to restore the default.

Syntax

[no] network-access dynamic-qos

Default Setting

Disabled

Command Mode

Interface Configuration

Command Usage

- ◆ The RADIUS server may optionally return dynamic QoS assignments to be applied to a switch port for an authenticated user. The “Filter-ID” attribute (attribute 11) can be configured on the RADIUS server to pass the following QoS information:

Table 55: Dynamic QoS Profiles

Profile	Attribute Syntax	Example
DiffServ	service-policy-in = <i>policy-map-name</i>	service-policy-in=p1
Rate Limit	rate-limit-input = <i>rate</i>	rate-limit-input=100 (Kbps)
802.1p	switchport-priority-default = <i>value</i>	switchport-priority-default=2
IP ACL	ip-access-group-in = <i>ip-acl-name</i>	ip-access-group-in=ip4acl
IPv6 ACL	ipv6-access-group-in = <i>ipv6-acl-name</i>	ipv6-access-group-in=ipv6acl
MAC ACL	mac-access-group-in = <i>mac-acl-name</i>	mac-access-group-in=macAcl

- ◆ When the last user logs off of a port with a dynamic QoS assignment, the switch restores the original QoS configuration for the port.
- ◆ When a user attempts to log into the network with a returned dynamic QoS profile that is different from users already logged on to the same port, the user is denied access.
- ◆ While a port has an assigned dynamic QoS profile, any manual QoS configuration changes only take effect after all users have logged off of the port.



Note: Any configuration changes for dynamic QoS are not saved to the switch configuration file.

Example

The following example enables the dynamic QoS feature on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access dynamic-qos
Console(config-if)#
```

network-access dynamic-vlan Use this command to enable dynamic VLAN assignment for an authenticated port. Use the **no** form to disable dynamic VLAN assignment.

Syntax

[no] network-access dynamic-vlan

Default Setting

Enabled

Command Mode

Interface Configuration

Command Usage

- ◆ When enabled, the VLAN identifiers returned by the RADIUS server through the 802.1X authentication process will be applied to the port, providing the VLANs have already been created on the switch. GVRP is not used to create the VLANs.
- ◆ The VLAN settings specified by the first authenticated MAC address are implemented for a port. Other authenticated MAC addresses on the port must have same VLAN configuration, or they are treated as an authentication failure.
- ◆ If dynamic VLAN assignment is enabled on a port and the RADIUS server returns no VLAN configuration, the authentication is still treated as a success, and the host assigned to the default untagged VLAN.
- ◆ When the dynamic VLAN assignment status is changed on a port, all authenticated addresses are cleared from the secure MAC address table.

Example

The following example enables dynamic VLAN assignment on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access dynamic-vlan
Console(config-if)#
```

network-access guest-vlan Use this command to assign all traffic on a port to a guest VLAN when 802.1x authentication is rejected. Use the **no** form of this command to disable guest VLAN assignment.

Syntax

network-access guest-vlan *vlan-id*

no network-access guest-vlan

vlan-id - VLAN ID (Range: 1-4094)

Default Setting

Disabled

Command Mode

Interface Configuration

Command Usage

- ◆ The VLAN to be used as the guest VLAN must be defined and set as active (See the [vlan database](#) command).
- ◆ When used with 802.1X authentication, the intrusion-action must be set for "guest-vlan" to be effective (see the [dot1x intrusion-action](#) command).

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access guest-vlan 25
Console(config-if)#
```

network-access link-detection Use this command to enable link detection for the selected port. Use the **no** form of this command to restore the default.

Syntax

[no] network-access link-detection

Default Setting

Disabled

Command Mode

Interface Configuration

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection
Console(config-if)#
```

network-access link-detection link-down Use this command to detect link-down events. When detected, the switch can shut down the port, send an SNMP trap, or both. Use the **no** form of this command to disable this feature.

Syntax

network-access link-detection link-down
action [shutdown | trap | trap-and-shutdown]

no network-access link-detection

action - Response to take when port security is violated.

shutdown - Disable port only.

trap - Issue SNMP trap message only.

trap-and-shutdown - Issue SNMP trap message and disable the port.

Default Setting

Disabled

Command Mode

Interface Configuration

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection link-down action trap
Console(config-if)#
```

network-access link-detection link-up Use this command to detect link-up events. When detected, the switch can shut down the port, send an SNMP trap, or both. Use the **no** form of this command to disable this feature.

Syntax

network-access link-detection link-up
action [shutdown | trap | trap-and-shutdown]

no network-access link-detection

action - Response to take when port security is violated.

shutdown - Disable port only.

trap - Issue SNMP trap message only.

trap-and-shutdown - Issue SNMP trap message and disable the port.

Default Setting

Disabled

Command Mode

Interface Configuration

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection link-up action trap
Console(config-if)#
```

network-access link-detection link-up-down Use this command to detect link-up and link-down events. When either event is detected, the switch can shut down the port, send an SNMP trap, or both. Use the **no** form of this command to disable this feature.

Syntax

network-access link-detection link-up-down
action [shutdown | trap | trap-and-shutdown]

no network-access link-detection

action - Response to take when port security is violated.

shutdown - Disable port only.

trap - Issue SNMP trap message only.

trap-and-shutdown - Issue SNMP trap message and disable the port.

Default Setting

Disabled

Command Mode

Interface Configuration

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection link-up-down action trap
Console(config-if)#
```

network-access max-mac-count Use this command to set the maximum number of MAC addresses that can be authenticated on a port interface via all forms of authentication. Use the **no** form of this command to restore the default.

Syntax

network-access max-mac-count *count*

no network-access max-mac-count

count - The maximum number of authenticated IEEE 802.1X and MAC addresses allowed. (Range: 0-1024; 0 for unlimited)

Default Setting

1024

Command Mode

Interface Configuration

Command Usage

The maximum number of MAC addresses per port is 1024, and the maximum number of secure MAC addresses supported for the switch system is 1024. When the limit is reached, all new MAC addresses are treated as authentication failures.

Example

```
Console(config-if)#network-access max-mac-count 5  
Console(config-if)#
```

network-access mode mac-authentication Use this command to enable network access authentication on a port. Use the **no** form of this command to disable network access authentication.

Syntax

[no] network-access mode mac-authentication

Default Setting

Disabled

Command Mode

Interface Configuration

Command Usage

- ◆ When enabled on a port, the authentication process sends a Password Authentication Protocol (PAP) request to a configured RADIUS server. The user name and password are both equal to the MAC address being authenticated.
- ◆ On the RADIUS server, PAP user name and passwords must be configured in the MAC address format XX-XX-XX-XX-XX-XX (all in upper case).
- ◆ Authenticated MAC addresses are stored as dynamic entries in the switch secure MAC address table and are removed when the aging time expires. The maximum number of secure MAC addresses supported for the switch system is 1024.
- ◆ Configured static MAC addresses are added to the secure address table when seen on a switch port. Static addresses are treated as authenticated without sending a request to a RADIUS server.
- ◆ MAC authentication, 802.1X, and port security cannot be configured together on the same port. Only one security mechanism can be applied.
- ◆ MAC authentication cannot be configured on trunk ports.

- ◆ When port status changes to down, all MAC addresses are cleared from the secure MAC address table. Static VLAN assignments are not restored.
- ◆ The RADIUS server may optionally return a VLAN identifier list. VLAN identifier list is carried in the "Tunnel-Private-Group-ID" attribute. The VLAN list can contain multiple VLAN identifiers in the format "1u,2t," where "u" indicates untagged VLAN and "t" tagged VLAN. The "Tunnel-Type" attribute should be set to "VLAN," and the "Tunnel-Medium-Type" attribute set to "802."

Example

```
Console(config-if)#network-access mode mac-authentication
Console(config-if)#
```

network-access port-mac-filter Use this command to enable the specified MAC address filter. Use the **no** form of this command to disable the specified MAC address filter.

Syntax

network-access port-mac-filter *filter-id*

no network-access port-mac-filter

filter-id - Specifies a MAC address filter table. (Range: 1-64)

Default Setting

None

Command Mode

Interface Configuration

Command Mode

- ◆ Entries in the MAC address filter table can be configured with the [network-access mac-filter](#) command.
- ◆ Only one filter table can be assigned to a port.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access port-mac-filter 1
Console(config-if)#
```

mac-authentication intrusion-action Use this command to configure the port response to a host MAC authentication failure. Use the **no** form of this command to restore the default.

Syntax

mac-authentication intrusion-action {block traffic | pass traffic}
no mac-authentication intrusion-action

Default Setting

Block Traffic

Command Mode

Interface Configuration

Example

```
Console(config-if)#mac-authentication intrusion-action block-traffic  
Console(config-if)#
```

mac-authentication max-mac-count Use this command to set the maximum number of MAC addresses that can be authenticated on a port via MAC authentication. Use the **no** form of this command to restore the default.

Syntax

mac-authentication max-mac-count *count*
no mac-authentication max-mac-count

count - The maximum number of MAC-authenticated MAC addresses allowed. (Range: 1-1024)

Default Setting

1024

Command Mode

Interface Configuration

Example

```
Console(config-if)#mac-authentication max-mac-count 32  
Console(config-if)#
```

clear network-access Use this command to clear entries from the secure MAC addresses table.

Syntax

clear network-access mac-address-table [**static** | **dynamic**]
[**address** *mac-address*] [**interface** *interface*]

static - Specifies static address entries.

dynamic - Specifies dynamic address entries.

mac-address - Specifies a MAC address entry. (Format: xx-xx-xx-xx-xx-xx)

interface - Specifies a port interface.

ethernet *unit/port*

unit - This is unit 1.

port - Port number. (Range: 1-52)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#clear network-access mac-address-table interface ethernet 1/1
Console#
```

show network-access Use this command to display the MAC authentication settings for port interfaces.

Syntax

show network-access [**interface** *interface*]

interface - Specifies a port interface.

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

Default Setting

Displays the settings for all interfaces.

Command Mode

Privileged Exec

Example

```
Console#show network-access interface ethernet 1/1
Global secure port information
Reauthentication Time                : 1800
MAC Address Aging                   : Enabled

Port : 1/1
MAC Authentication                   : Disabled
MAC Authentication Intrusion Action  : Block traffic
MAC Authentication Maximum MAC Counts : 1024
Maximum MAC Counts                   : 2048
Dynamic VLAN Assignment              : Enabled
Dynamic QoS Assignment               : Disabled
MAC Filter ID                       : Disabled
Guest VLAN                           : Disabled
Link Detection                       : Disabled
Detection Mode                       : Link-down
Detection Action                     : Trap
Console#
```

show network-access mac-address-table Use this command to display secure MAC address table entries.

Syntax

show network-access mac-address-table [**static** | **dynamic**]
[**address** *mac-address* [*mask*]] [**interface** *interface*] [**sort** {**address** |
interface}]

static - Specifies static address entries.

dynamic - Specifies dynamic address entries.

mac-address - Specifies a MAC address entry. (Format: xx-xx-xx-xx-xx-xx)

mask - Specifies a MAC address bit mask for filtering displayed addresses.

interface - Specifies a port interface.

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

sort - Sorts displayed entries by either MAC address or interface.

Default Setting

Displays all filters.

Command Mode

Privileged Exec

Command Usage

When using a bit mask to filter displayed MAC addresses, a 1 means “care” and a 0 means “don't care”. For example, a MAC of 00-00-01-02-03-04 and mask FF-FF-FF-

00-00-00 would result in all MACs in the range 00-00-01-00-00-00 to 00-00-01-FF-FF-FF to be displayed. All other MACs would be filtered out.

Example

```
Console#show network-access mac-address-table
-----
Port  MAC-Address      RADIUS-Server  Attribute  Time
-----
1/1   00-00-01-02-03-04  172.155.120.17 Static      00d06h32m50s
1/1   00-00-01-02-03-05  172.155.120.17 Dynamic    00d06h33m20s
1/1   00-00-01-02-03-06  172.155.120.17 Static      00d06h35m10s
1/3   00-00-01-02-03-07  172.155.120.17 Dynamic    00d06h34m20s

Console#
```

show network-access mac-filter Use this command to display information for entries in the MAC filter tables.

Syntax

show network-access mac-filter [*filter-id*]

filter-id - Specifies a MAC address filter table. (Range: 1-64)

Default Setting

Displays all filters.

Command Mode

Privileged Exec

Example

```
Console#show network-access mac-filter
Filter ID  MAC Address      MAC Mask
-----
1  00-00-01-02-03-08  FF-FF-FF-FF-FF-FF

Console#
```

Web Authentication

Web authentication allows stations to authenticate and access the network in situations where 802.1X or Network Access authentication are infeasible or impractical. The web authentication feature allows unauthenticated hosts to request and receive a DHCP assigned IP address and perform DNS queries. All other traffic, except for HTTP protocol traffic, is blocked. The switch intercepts HTTP protocol traffic and redirects it to a switch-generated web page that facilitates user name and password authentication via RADIUS. Once authentication is successful, the web browser is forwarded on to the originally requested web page. Successful authentication is valid for all hosts connected to the port.



Note: RADIUS authentication must be activated and configured for the web authentication feature to work properly (see [“Authentication Sequence” on page 220](#)).

Note: Web authentication cannot be configured on trunk ports.

Table 56: Web Authentication

Command	Function	Mode
web-auth login-attempts	Defines the limit for failed web authentication login attempts	GC
web-auth quiet-period	Defines the amount of time to wait after the limit for failed login attempts is exceeded.	GC
web-auth session-timeout	Defines the amount of time a session remains valid	GC
web-auth system-auth-control	Enables web authentication globally for the switch	GC
web-auth	Enables web authentication for an interface	IC
web-auth re-authenticate (Port)	Ends all web authentication sessions on the port and forces the users to re-authenticate	PE
web-auth re-authenticate (IP)	Ends the web authentication session associated with the designated IP address and forces the user to re-authenticate	PE
show web-auth	Displays global web authentication parameters	PE
show web-auth interface	Displays interface-specific web authentication parameters and statistics	PE
show web-auth summary	Displays a summary of web authentication port parameters and statistics	PE

web-auth login-attempts

This command defines the limit for failed web authentication login attempts. After the limit is reached, the switch refuses further login attempts until the quiet time expires. Use the **no** form to restore the default.

Syntax

web-auth login-attempts *count*

no web-auth login-attempts

count - The limit of allowed failed login attempts. (Range: 1-3)

Default Setting

3 login attempts

Command Mode

Global Configuration

Example

```
Console(config)#web-auth login-attempts 2
Console(config)#
```

web-auth quiet-period This command defines the amount of time a host must wait after exceeding the limit for failed login attempts, before it may attempt web authentication again. Use the **no** form to restore the default.

Syntax

web-auth quiet-period *time*

no web-auth quiet period

time - The amount of time the host must wait before attempting authentication again. (Range: 1-180 seconds)

Default Setting

60 seconds

Command Mode

Global Configuration

Example

```
Console(config)#web-auth quiet-period 120
Console(config)#
```

web-auth session-timeout This command defines the amount of time a web-authentication session remains valid. When the session timeout has been reached, the host is logged off and must re-authenticate itself the next time data transmission takes place. Use the **no** form to restore the default.

Syntax

web-auth session-timeout *timeout*

no web-auth session timeout

timeout - The amount of time that an authenticated session remains valid. (Range: 300-3600 seconds)

Default Setting

3600 seconds

Command Mode

Global Configuration

Example

```
Console(config)#web-auth session-timeout 1800
Console(config)#
```

web-auth system-auth-control This command globally enables web authentication for the switch. Use the **no** form to restore the default.

Syntax

[no] web-auth system-auth-control

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

Both **web-auth system-auth-control** for the switch and **web-auth** for an interface must be enabled for the web authentication feature to be active.

Example

```
Console(config)#web-auth system-auth-control
Console(config)#
```

web-auth This command enables web authentication for an interface. Use the **no** form to restore the default.

Syntax

[no] web-auth

Default Setting

Disabled

Command Mode

Interface Configuration

Command Usage

Both **web-auth system-auth-control** for the switch and **web-auth** for a port must be enabled for the web authentication feature to be active.

Example

```
Console(config-if)#web-auth  
Console(config-if)#
```

web-auth re-authenticate (Port) This command ends all web authentication sessions connected to the port and forces the users to re-authenticate.

Syntax

web-auth re-authenticate interface *interface*

interface - Specifies a port interface.

ethernet *unit/port*

unit - This is unit 1.

port - Port number. (Range: 1-52)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#web-auth re-authenticate interface ethernet 1/2  
Console#
```

web-auth re-authenticate (IP) This command ends the web authentication session associated with the designated IP address and forces the user to re-authenticate.

Syntax

web-auth re-authenticate interface *interface ip*

interface - Specifies a port interface.

ethernet *unit/port*

unit - This is unit 1.

port - Port number. (Range: 1-52)

ip - IPv4 formatted IP address

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#web-auth re-authenticate interface ethernet 1/2 192.168.1.5
Console#
```

show web-auth This command displays global web authentication parameters.

Command Mode

Privileged Exec

Example

```
Console#show web-auth
Global Web-Auth Parameters
  System Auth Control      : Enabled
  Session Timeout          : 3600
  Quiet Period             : 60
  Max Login Attempts       : 3
Console#
```

show web-auth interface This command displays interface-specific web authentication parameters and statistics.

Syntax

show web-auth interface *interface*

interface - Specifies a port interface.

ethernet *unit/port*

unit - This is unit 1.

port - Port number. (Range: 1-52)

Command Mode

Privileged Exec

Example

```
Console#show web-auth interface ethernet 1/2
Web Auth Status      : Enabled

Host Summary

IP address      Web-Auth-State  Remaining-Session-Time
-----
1.1.1.1         Authenticated   295
1.1.1.2         Authenticated   111
Console#
```

show web-auth summary This command displays a summary of web authentication port parameters and statistics.

Command Mode
Privileged Exec

Example

```
Console#show web-auth summary
Global Web-Auth Parameters
  System Auth Control      : Enabled
Port      Status          Authenticated Host Count
----      -
1/ 1      Disabled        0
1/ 2      Enabled         8
1/ 3      Disabled        0
1/ 4      Disabled        0
1/ 5      Disabled        0
:
```

DHCPv4 Snooping

DHCP snooping allows a switch to protect a network from rogue DHCP servers or other devices which send port-related information to a DHCP server. This information can be useful in tracking an IP address back to a physical port. This section describes commands used to configure DHCP snooping.

Table 57: DHCP Snooping Commands

Command	Function	Mode
ip dhcp snooping	Enables DHCP snooping globally	GC
ip dhcp snooping information option	Enables or disables the use of DHCP Option 82 information, and specifies frame format for the remote-id	GC
ip dhcp snooping information policy	Sets the information option policy for DHCP client packets that include Option 82 information	GC
ip dhcp snooping verify mac-address	Verifies the client's hardware address stored in the DHCP packet against the source MAC address in the Ethernet header	GC
ip dhcp snooping vlan	Enables DHCP snooping on the specified VLAN	GC
ip dhcp snooping information option circuit-id	Enables or disables the use of DHCP Option 82 information circuit-id suboption	IC
ip dhcp snooping trust	Configures the specified interface as trusted	IC
clear ip dhcp snooping binding	Clears DHCP snooping binding table entries from RAM	PE
clear ip dhcp snooping database flash	Removes all dynamically learned snooping entries from flash memory.	PE
ip dhcp snooping database flash	Writes all dynamically learned snooping entries to flash memory	PE

Table 57: DHCP Snooping Commands (Continued)

Command	Function	Mode
<code>show ip dhcp snooping</code>	Shows the DHCP snooping configuration settings	PE
<code>show ip dhcp snooping binding</code>	Shows the DHCP snooping binding table entries	PE

ip dhcp snooping This command enables DHCP snooping globally. Use the **no** form to restore the default setting.

Syntax

[no] ip dhcp snooping

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ Network traffic may be disrupted when malicious DHCP messages are received from an outside source. DHCP snooping is used to filter DHCP messages received on an unsecure interface from outside the network or fire wall. When DHCP snooping is enabled globally by this command, and enabled on a VLAN interface by the `ip dhcp snooping vlan` command, DHCP messages received on an untrusted interface (as specified by the `no ip dhcp snooping trust` command) from a device not listed in the DHCP snooping table will be dropped.
- ◆ When enabled, DHCP messages entering an untrusted interface are filtered based upon dynamic entries learned via DHCP snooping.
- ◆ Table entries are only learned for trusted interfaces. Each entry includes a MAC address, IP address, lease time, VLAN identifier, and port identifier.
- ◆ When DHCP snooping is enabled, the rate limit for the number of DHCP messages that can be processed by the switch is 100 packets per second. Any DHCP packets in excess of this limit are dropped.
- ◆ Filtering rules are implemented as follows:
 - If the global DHCP snooping is disabled, all DHCP packets are forwarded.
 - If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, all DHCP packets are forwarded for a *trusted* port. If the received packet is a DHCP ACK message, a dynamic DHCP snooping entry is also added to the binding table.

- If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, but the port is *not trusted*, it is processed as follows:
 - If the DHCP packet is a reply packet from a DHCP server (including OFFER, ACK or NAK messages), the packet is dropped.
 - If the DHCP packet is from a client, such as a DECLINE or RELEASE message, the switch forwards the packet only if the corresponding entry is found in the binding table.
 - If the DHCP packet is from client, such as a DISCOVER, REQUEST, INFORM, DECLINE or RELEASE message, the packet is forwarded if MAC address verification is disabled (as specified by the [ip dhcp snooping verify mac-address](#) command). However, if MAC address verification is enabled, then the packet will only be forwarded if the client's hardware address stored in the DHCP packet is the same as the source MAC address in the Ethernet header.
 - If the DHCP packet is not a recognizable type, it is dropped.
- If a DHCP packet from a client passes the filtering criteria above, it will only be forwarded to trusted ports in the same VLAN.
- If a DHCP packet is from server is received on a trusted port, it will be forwarded to both trusted and untrusted ports in the same VLAN.
- ◆ If the DHCP snooping is globally disabled, all dynamic bindings are removed from the binding table.
- ◆ *Additional considerations when the switch itself is a DHCP client* – The port(s) through which the switch submits a client request to the DHCP server must be configured as trusted (using the [ip dhcp snooping trust](#) command). Note that the switch will not add a dynamic entry for itself to the binding table when it receives an ACK message from a DHCP server. Also, when the switch sends out DHCP client packets for itself, no filtering takes place. However, when the switch receives any messages from a DHCP server, any packets received from untrusted ports are dropped.

Example

This example enables DHCP snooping globally for the switch.

```
Console(config)#ip dhcp snooping
Console(config)#
```

Related Commands

[ip dhcp snooping vlan \(306\)](#)
[ip dhcp snooping trust \(308\)](#)

ip dhcp snooping information option

This command enables the use of DHCP Option 82 information for the switch, and specifies the frame format to use for the remote-id when Option 82 information is generated by the switch. Use the **no** form without any keywords to disable this function, the **no** form with the **encode no-subtype** keyword to enable use of sub-type and sub-length in CID/RID fields, or the **no** form with the **remote-id** keyword to set the remote ID to the switch's MAC address encoded in hexadecimal.

Syntax

ip dhcp snooping information option

```
[encode no-subtype]
[remote-id {ip-address [encode {ascii | hex}] |
mac-address [encode {ascii | hex}] |
string string}]
```

no ip dhcp snooping information option

```
[encode no-subtype]
[remote-id [ip-address encode] | [mac-address encode]]
```

encode no-subtype - Disables use of sub-type and sub-length fields in circuit-ID (CID) and remote-ID (RID) in Option 82 information.

mac-address - Inserts a MAC address in the remote ID sub-option for the DHCP snooping agent (that is, the MAC address of the switch's CPU).

ip-address - Inserts an IP address in the remote ID sub-option for the DHCP snooping agent (that is, the IP address of the management interface).

encode - Indicates encoding in ASCII or hexadecimal.

string - An arbitrary string inserted into the remote identifier field.
(Range: 1-32 characters)

Default Setting

Option 82: Disabled

CID/RID sub-type: Enabled

Remote ID: MAC address (hexadecimal)

Command Mode

Global Configuration

Command Usage

- ◆ DHCP provides a relay mechanism for sending information about the switch and its DHCP clients to the DHCP server. Known as DHCP Option 82, it allows compatible DHCP servers to use the information when assigning IP addresses, or to set other services or policies for clients.
- ◆ When the DHCP Snooping Information Option 82 is enabled, the requesting client (or an intermediate relay agent that has used the information fields to describe itself) can be identified in the DHCP request packets forwarded by the switch and in reply packets sent back from the DHCP server.

- ◆ When the DHCP Snooping Information Option is enabled, clients can be identified by the switch port to which they are connected rather than just their MAC address. DHCP client-server exchange messages are then forwarded directly between the server and client without having to flood them to the entire VLAN.
- ◆ DHCP snooping must be enabled for the DHCP Option 82 information to be inserted into packets. When enabled, the switch will only add/remove option 82 information in incoming DHCP packets but not relay them. Packets are processed as follows:
 - If an incoming packet is a DHCP request packet with option 82 information, it will modify the option 82 information according to settings specified with `ip dhcp snooping information policy` command.
 - If an incoming packet is a DHCP request packet without option 82 information, enabling the DHCP snooping information option will add option 82 information to the packet.
 - If an incoming packet is a DHCP reply packet with option 82 information, enabling the DHCP snooping information option will remove option 82 information from the packet.

Example

This example enables the DHCP Snooping Information Option.

```
Console(config)#ip dhcp snooping information option
Console(config)#
```

ip dhcp snooping information policy

This command sets the DHCP snooping information option policy for DHCP client packets that include Option 82 information.

Syntax

ip dhcp snooping information policy {drop | keep | replace}

drop - Drops the client's request packet instead of relaying it.

keep - Retains the Option 82 information in the client request, and forwards the packets to trusted ports.

replace - Replaces the Option 82 information circuit-id and remote-id fields in the client's request with information about the relay agent itself, inserts the relay agent's address (when DHCP snooping is enabled), and forwards the packets to trusted ports.

Default Setting

replace

Command Mode

Global Configuration

Command Usage

When the switch receives DHCP packets from clients that already include DHCP Option 82 information, the switch can be configured to set the action policy for these packets. The switch can either drop the DHCP packets, keep the existing information, or replace it with the switch's relay information.

Example

```
Console(config)#ip dhcp snooping information policy drop
Console(config)#
```

ip dhcp snooping verify mac-address

This command verifies the client's hardware address stored in the DHCP packet against the source MAC address in the Ethernet header. Use the **no** form to disable this function.

Syntax

[no] ip dhcp binding verify mac-address

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

If MAC address verification is enabled, and the source MAC address in the Ethernet header of the packet is not same as the client's hardware address in the DHCP packet, the packet is dropped.

Example

This example enables MAC address verification.

```
Console(config)#ip dhcp snooping verify mac-address
Console(config)#
```

Related Commands

[ip dhcp snooping \(301\)](#)

[ip dhcp snooping vlan \(306\)](#)

[ip dhcp snooping trust \(308\)](#)

ip dhcp snooping vlan This command enables DHCP snooping on the specified VLAN. Use the **no** form to restore the default setting.

Syntax

[no] ip dhcp snooping vlan *vlan-id*

vlan-id - ID of a configured VLAN (Range: 1-4094)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ When DHCP snooping is enabled globally using the [ip dhcp snooping](#) command, and enabled on a VLAN with this command, DHCP packet filtering will be performed on any untrusted ports within the VLAN as specified by the [ip dhcp snooping trust](#) command.
- ◆ When the DHCP snooping is globally disabled, DHCP snooping can still be configured for specific VLANs, but the changes will not take effect until DHCP snooping is globally re-enabled.
- ◆ When DHCP snooping is globally enabled, and DHCP snooping is then disabled on a specific VLAN, all dynamic bindings learned for this VLAN are removed from the binding table.

Example

This example enables DHCP snooping for VLAN 1.

```
Console(config)#ip dhcp snooping vlan 1
Console(config)#
```

Related Commands

[ip dhcp snooping \(301\)](#)

[ip dhcp snooping trust \(308\)](#)

ip dhcp snooping information option circuit-id This command enables the use of DHCP Option 82 information circuit-id suboption. Use the **no** form to disable this feature.

Syntax

ip dhcp snooping information option circuit-id string *string*

no dhcp snooping information option circuit-id

string - An arbitrary string inserted into the circuit identifier field.
(Range: 1-32 characters)

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ DHCP provides a relay mechanism for sending information about the switch and its DHCP clients to the DHCP server. DHCP Option 82 allows compatible DHCP servers to use the information when assigning IP addresses, to set other services or policies for clients. For more information of this process, refer to the Command Usage section under the [ip dhcp snooping information option](#) command.
- ◆ Option 82 information generated by the switch is based on TR-101 syntax as shown below:

Table 58: Option 82 information

82	3-69	1	1-67	x1	x2	x3	x4	x5	x63
opt82	opt-len	sub-opt1	string-len						R-124 string

The circuit identifier used by this switch starts at sub-option1 and goes to the end of the R-124 string. The R-124 string includes the following information:

- sub-type - Distinguishes different types of circuit IDs.
- sub-length - Length of the circuit ID type
- access node identifier - ASCII string. Default is the MAC address of the switch's CPU. This field is set by the [ip dhcp snooping information option](#) command,
- eth - The second field is the fixed string "eth"
- slot - The slot represents the stack unit for this system.
- port - The port which received the DHCP request. If the packet arrives over a trunk, the value is the ifIndex of the trunk.

- **vlan** - Tag of the VLAN which received the DHCP request.

Note that the sub-type and sub-length fields can be enabled or disabled using the [ip dhcp snooping information option](#) command.

- The **ip dhcp snooping information option circuit-id** command can be used to modify the default settings described above.

Example

This example sets the DHCP Snooping Information circuit-id suboption string.

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip dhcp snooping information option circuit-id string 4500
Console(config-if)#
```

ip dhcp snooping trust This command configures the specified interface as trusted. Use the **no** form to restore the default setting.

Syntax

[no] ip dhcp snooping trust

Default Setting

All interfaces are untrusted

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ A trusted interface is an interface that is configured to receive only messages from within the network. An untrusted interface is an interface that is configured to receive messages from outside the network or fire wall.
- ◆ Set all ports connected to DHCP servers within the local network or fire wall to trusted, and all other ports outside the local network or fire wall to untrusted.
- ◆ When DHCP snooping is enabled globally using the [ip dhcp snooping](#) command, and enabled on a VLAN with [ip dhcp snooping vlan](#) command, DHCP packet filtering will be performed on any untrusted ports within the VLAN according to the default status, or as specifically configured for an interface with the **no ip dhcp snooping trust** command.
- ◆ When an untrusted port is changed to a trusted port, all the dynamic DHCP snooping bindings associated with this port are removed.
- ◆ *Additional considerations when the switch itself is a DHCP client* – The port(s) through which it submits a client request to the DHCP server must be configured as trusted.

Example

This example sets port 5 to untrusted.

```
Console(config)#interface ethernet 1/5
Console(config-if)#no ip dhcp snooping trust
Console(config-if)#
```

Related Commands

[ip dhcp snooping \(301\)](#)

[ip dhcp snooping vlan \(306\)](#)

clear ip dhcp snooping binding

This command clears DHCP snooping binding table entries from RAM. Use this command without any optional keywords to clear all entries from the binding table.

Syntax

clear ip dhcp snooping binding [*mac-address* **vlan** *vlan-id*]

mac-address - Specifies a MAC address entry.

(Format: xx-xx-xx-xx-xx-xx)

vlan-id - ID of a configured VLAN (Range: 1-4094)

Command Mode

Privileged Exec

Example

```
Console(config)#clear ip dhcp snooping binding 11-22-33-44-55-66 vlan 1
Console(config)#
```

clear ip dhcp snooping database flash

This command removes all dynamically learned snooping entries from flash memory.

Command Mode

Privileged Exec

Example

```
Console(config)#ip dhcp snooping database flash
Console(config)#
```

ip dhcp snooping database flash This command writes all dynamically learned snooping entries to flash memory.

Command Mode
Privileged Exec

Command Usage

This command can be used to store the currently learned dynamic DHCP snooping entries to flash memory. These entries will be restored to the snooping table when the switch is reset. However, note that the lease time shown for a dynamic entry that has been restored from flash memory will no longer be valid.

Example

```
Console#clear ip dhcp snooping database flash
Console#
```

show ip dhcp snooping This command shows the DHCP snooping configuration settings.

Command Mode
Privileged Exec

Example

```
Console#show ip dhcp snooping
Global DHCP Snooping Status: disable
DHCP Snooping Information Option Status: disable
DHCP Snooping Information Policy: replace
DHCP Snooping is configured on the following VLANs:
1
Verify Source MAC-Address: enable
Interface          Trusted
-----
Eth 1/1            No
Eth 1/2            No
Eth 1/3            No
Eth 1/4            No
Eth 1/5            Yes
.
.
.
```

show ip dhcp snooping binding This command shows the DHCP snooping binding table entries.

Command Mode
Privileged Exec

Example

```
Console#show ip dhcp snooping binding
MAC Address      IP Address      Lease(sec)  Type           VLAN  Interface
-----
11-22-33-44-55-66 192.168.0.99    0          Dynamic-DHCPSNP 1     Eth 1/5
Console#
```

DHCPv6 Snooping

DHCPv6 snooping allows a switch to protect a network from rogue DHCPv6 servers or other devices which send port-related information to a DHCPv6 server. This information can be useful in tracking an IP address back to a physical port. This section describes commands used to configure DHCPv6 snooping.

Table 59: DHCP Snooping Commands

Command	Function	Mode
ipv6 dhcp snooping	Enables DHCPv6 snooping globally	GC
ipv6 dhcp snooping vlan	Enables DHCPv6 snooping on the specified VLAN	GC
ipv6 dhcp snooping max-binding	Sets the maximum number of entries which can be stored in the binding database for an interface	IC
ipv6 dhcp snooping trust	Configures the specified interface as trusted	IC
clear ipv6 dhcp snooping binding	Clears DHCPv6 snooping binding table entries from RAM	PE
clear ipv6 dhcp snooping statistics	Clears statistical counters for DHCPv6 snooping client, server and relay packets	PE
show ipv6 dhcp snooping	Shows the DHCPv6 snooping configuration settings	PE
show ipv6 dhcp snooping binding	Shows the DHCPv6 snooping binding table entries	PE
show ipv6 dhcp snooping statistics	Shows statistics for DHCPv6 snooping client, server and relay packets	PE

ipv6 dhcp snooping This command enables DHCPv6 snooping globally. Use the **no** form to restore the default setting.

Syntax

[no] ipv6 dhcp snooping

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ Network traffic may be disrupted when malicious DHCPv6 messages are received from an outside source. DHCPv6 snooping is used to filter DHCPv6 messages received on an unsecure interface from outside the network or fire wall. When DHCPv6 snooping is enabled globally by this command, and enabled on a VLAN interface by the [ipv6 dhcp snooping vlan](#) command, DHCP messages received on an untrusted interface (as specified by the [no ipv6 dhcp snooping trust](#) command) from a device not listed in the DHCPv6 snooping table will be dropped.
- ◆ When enabled, DHCPv6 messages entering an untrusted interface are filtered based upon dynamic entries learned via DHCPv6 snooping.
- ◆ Table entries are only learned for trusted interfaces. Each entry includes a MAC address, IPv6 address, lease time, binding type, VLAN identifier, and port identifier.
- ◆ When DHCPv6 snooping is enabled, the rate limit for the number of DHCPv6 messages that can be processed by the switch is 100 packets per second. Any DHCPv6 packets in excess of this limit are dropped.
- ◆ Filtering rules are implemented as follows:
 - If global DHCPv6 snooping is disabled, all DHCPv6 packets are forwarded.
 - If DHCPv6 snooping is enabled globally, and also enabled on the VLAN where the DHCPv6 packet is received, DHCPv6 packets are forwarded for a *trusted* port as described below.
 - If DHCPv6 snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, but the port is *not trusted*, DHCP packets are processed according to message type as follows:

DHCP Client Packet

- Request: Update entry in binding cache, recording client's DHCPv6 Unique Identifier (DUID), server's DUID, Identity Association (IA) type, IA

Identifier, and address (4 message exchanges to get IPv6 address), and forward to trusted port.

- Solicit: Add new entry in binding cache, recording client's DUID, IA type, IA ID (2 message exchanges to get IPv6 address with rapid commit option, otherwise 4 message exchanges), and forward to trusted port.
- Decline: If no matching entry is found in binding cache, drop this packet.
- Renew, Rebind, Release, Confirm: If no matching entry is found in binding cache, drop this packet.
- If the DHCPv6 packet is not a recognizable type, it is dropped.

If a DHCPv6 packet from a client passes the filtering criteria above, it will only be forwarded to trusted ports in the same VLAN.

DHCP Server Packet

- If a DHCP server packet is received on an *untrusted* port, drop this packet and add a log entry in the system.
- If a DHCPv6 Reply packet is received from a server on a *trusted* port, it will be processed in the following manner:
 - A.** Check if IPv6 address in IA option is found in binding table:
 - If yes, continue to C.
 - If not, continue to B.
 - B.** Check if IPv6 address in IA option is found in binding cache:
 - If yes, continue to C.
 - If not, check failed, and forward packet to trusted port.
 - C.** Check status code in IA option:
 - If successful, and entry is in binding table, update lease time and forward to original destination.
 - If successful, and entry is in binding cache, move entry from binding cache to binding table, update lease time and forward to original destination.
 - Otherwise, remove binding entry. and check failed.
- If a DHCPv6 Relay packet is received, check the relay message option in Relay-Forward or Relay-Reply packet, and process client and server packets as described above.

- ◆ If DHCPv6 snooping is globally disabled, all dynamic bindings are removed from the binding table.
- ◆ *Additional considerations when the switch itself is a DHCPv6 client* – The port(s) through which the switch submits a client request to the DHCPv6 server must be configured as trusted (using the [ipv6 dhcp snooping trust](#) command). Note that the switch will not add a dynamic entry for itself to the binding table when it receives an ACK message from a DHCPv6 server. Also, when the switch sends out DHCPv6 client packets for itself, no filtering takes place. However, when the switch receives any messages from a DHCPv6 server, any packets received from untrusted ports are dropped.

Example

This example enables DHCPv6 snooping globally for the switch.

```
Console(config)#ipv6 dhcp snooping
Console(config)#
```

Related Commands

[ipv6 dhcp snooping vlan \(314\)](#)

[ipv6 dhcp snooping trust \(315\)](#)

ipv6 dhcp snooping vlan This command enables DHCPv6 snooping on the specified VLAN. Use the **no** form to restore the default setting.

Syntax

[no] ipv6 dhcp snooping vlan {*vlan-id* | *vlan-range*}

vlan-id - ID of a configured VLAN (Range: 1-4094)

vlan-range - A consecutive range of VLANs indicated by the use a hyphen, or a random group of VLANs with each entry separated by a comma.

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ When DHCPv6 snooping enabled globally using the [ipv6 dhcp snooping](#) command, and enabled on a VLAN with this command, DHCPv6 packet filtering will be performed on any untrusted ports within the VLAN as specified by the [ipv6 dhcp snooping trust](#) command.
- ◆ When the DHCPv6 snooping is globally disabled, DHCPv6 snooping can still be configured for specific VLANs, but the changes will not take effect until DHCPv6 snooping is globally re-enabled.

- ◆ When DHCPv6 snooping is enabled globally, and then disabled on a VLAN, all dynamic bindings learned for this VLAN are removed from the binding table.

Example

This example enables DHCP6 snooping for VLAN 1.

```
Console(config)#ipv6 dhcp snooping vlan 1
Console(config)#
```

Related Commands

[ipv6 dhcp snooping \(312\)](#)

[ipv6 dhcp snooping trust \(315\)](#)

ipv6 dhcp snooping max-binding This command sets the maximum number of entries which can be stored in the binding database for an interface. Use the **no** form to restore the default setting.

Syntax

ipv6 dhcp snooping max-binding *count*

no ipv6 dhcp snooping max-binding

count - Maximum number of entries. (Range: 1-5)

Default Setting

5

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

This example sets the maximum number of binding entries to 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#ipv6 dhcp snooping max-binding 1
Console(config-if)#
```

ipv6 dhcp snooping trust This command configures the specified interface as trusted. Use the **no** form to restore the default setting.

Syntax

[no] ipv6 dhcp snooping trust

Default Setting

All interfaces are untrusted

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ A trusted interface is an interface that is configured to receive only messages from within the network. An untrusted interface is an interface that is configured to receive messages from outside the network or fire wall.
- ◆ Set all ports connected to DHCPv6 servers within the local network or fire wall to trusted, and all other ports outside the local network or fire wall to untrusted.
- ◆ When DHCPv6 snooping is enabled globally using the [ipv6 dhcp snooping](#) command, and enabled on a VLAN with [ipv6 dhcp snooping vlan](#) command, DHCPv6 packet filtering will be performed on any untrusted ports within the VLAN according to the default status, or as specifically configured for an interface with the **no ipv6 dhcp snooping trust** command.
- ◆ When an untrusted port is changed to a trusted port, all the dynamic DHCPv6 snooping bindings associated with this port are removed.
- ◆ *Additional considerations when the switch itself is a DHCPv6 client* – The port(s) through which it submits a client request to the DHCPv6 server must be configured as trusted.

Example

This example sets port 5 to untrusted.

```
Console(config)#interface ethernet 1/5
Console(config-if)#no ipv6 dhcp snooping trust
Console(config-if)#
```

Related Commands

[ipv6 dhcp snooping \(312\)](#)

[ipv6 dhcp snooping vlan \(314\)](#)

clear ipv6 dhcp snooping binding This command clears DHCPv6 snooping binding table entries from RAM. Use this command without any optional keywords to clear all entries from the binding table.

Syntax

clear ipv6 dhcp snooping binding [*mac-address* *ipv6-address*]

mac-address - Specifies a MAC address entry. (Format: xx-xx-xx-xx-xx-xx)

ipv6-address - Corresponding IPv6 address. This address must be entered according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

Command Mode

Privileged Exec

Example

```
Console(config)#clear ipv6 dhcp snooping binding 00-12-cf-01-02-03 2001::1
Console(config)#
```

clear ipv6 dhcp snooping statistics This command clears statistical counters for DHCPv6 snooping client, server and relay packets.

Command Mode

Privileged Exec

Example

```
Console(config)#clear ipv6 dhcp snooping statistics
Console(config)#
```

show ipv6 dhcp snooping This command shows the DHCPv6 snooping configuration settings.

Command Mode
Privileged Exec

Example

```
Console#show ipv6 dhcp snooping
Global DHCPv6 Snooping status: disabled
DHCPv6 Snooping is configured on the following VLANs:
1,
Interface          Trusted          Max-binding    Current-binding
-----
Eth 1/1             No               5              0
Eth 1/2             No               5              0
Eth 1/3             No               5              0
Eth 1/4             No               5              0
Eth 1/5             Yes              5              0
.
.
```

show ipv6 dhcp snooping binding This command shows the DHCPv6 snooping binding table entries.

Command Mode
Privileged Exec

Example

```
Console#show ipv6 dhcp snooping binding
NA - Non-temporary address
TA - Temporary address
-----
Link-layer Address: 00-13-49-aa-39-26
IPv6 Address          Lifetime    VLAN Port    Type
-----
2001:b021:1435:5612:ab3c:6792:a452:6712    2591998    1 Eth 1/5    NA
-----
Link-layer Address: 00-12-cf-01-02-03
IPv6 Address          Lifetime    VLAN Port    Type
-----
2001:b000::1          2591912    1 Eth 1/3    NA
Console#
```

show ipv6 dhcp snooping statistics This command shows statistics for DHCPv6 snooping client, server and relay packets.

Command Mode
Privileged Exec

Example

```

Console#show ipv6 dhcp snooping statistics
DHCPv6 Snooping Statistics:
  Client Packet: Solicit, Request, Confirm, Renew, Rebind,
                  Decline, Release, Information-request
  Server Packet: Advertise, Reply, Reconfigure
  Relay Packet: Relay-forward, Relay-reply
State      Client      Server      Relay      Total
-----
Received   10           9           0          19
Sent       9           9           0          18
Dropped    1           0           0           1

Console#

```

IPv4 Source Guard

IPv4 Source Guard is a security feature that filters IPv4 traffic on network interfaces based on manually configured entries in the IPv4 Source Guard table, or dynamic entries in the DHCPv4 Snooping table when enabled (see [“DHCPv4 Snooping” on page 300](#)). IPv4 source guard can be used to prevent traffic attacks caused when a host tries to use the IPv4 address of a neighbor to access the network. This section describes commands used to configure IPv4 Source Guard.

Table 60: IPv4 Source Guard Commands

Command	Function	Mode
ip source-guard binding	Adds a static address to the source-guard binding table	GC
ip source-guard	Configures the switch to filter inbound traffic based on source IP address, or source IP address and corresponding MAC address	IC
ip source-guard max-binding	Sets the maximum number of entries that can be bound to an interface	IC
show ip source-guard	Shows whether source guard is enabled or disabled on each interface	PE
show ip source-guard binding	Shows the source guard binding table	PE

ip source-guard binding This command adds a static address to the source-guard binding table. Use the **no** form to remove a static entry.

Syntax

ip source-guard binding *mac-address* **vlan** *vlan-id* *ip-address*
interface ethernet *unit/port*

no ip source-guard binding *mac-address* **vlan** *vlan-id*

mac-address - A valid unicast MAC address.

vlan-id - ID of a configured VLAN (Range: 1-4094)

ip-address - A valid unicast IP address, including classful types A, B or C.

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

Default Setting

No configured entries

Command Mode

Global Configuration

Command Usage

- ◆ Table entries include a MAC address, IP address, lease time, entry type (Static-IP-SG-Binding, Dynamic-DHCP-Binding), VLAN identifier, and port identifier.
- ◆ All static entries are configured with an infinite lease time, which is indicated with a value of zero by the [show ip source-guard](#) command.
- ◆ When source guard is enabled, traffic is filtered based upon dynamic entries learned via DHCP snooping, or static addresses configured in the source guard binding table with this command.
- ◆ Static bindings are processed as follows:
 - If there is no entry with same VLAN ID and MAC address, a new entry is added to binding table using the type of static IP source guard binding.
 - If there is an entry with same VLAN ID and MAC address, and the type of entry is static IP source guard binding, then the new entry will replace the old one.
 - If there is an entry with same VLAN ID and MAC address, and the type of the entry is dynamic DHCP snooping binding, then the new entry will replace the old one and the entry type will be changed to static IP source guard binding.

Example

This example configures a static source-guard binding on port 5.

```
Console(config)#ip source-guard binding 00-ab-11-cd-23-45 vlan 1 192.168.0.99
interface ethernet 1/5
Console(config)#
```

Related Commands

[ip source-guard \(321\)](#)

[ip dhcp snooping \(301\)](#)

[ip dhcp snooping vlan \(306\)](#)

ip source-guard This command configures the switch to filter inbound traffic based on source IP address, or source IP address and corresponding MAC address. Use the **no** form to disable this function.

Syntax

ip source-guard {sip | sip-mac}

no ip source-guard

sip - Filters traffic based on IP addresses stored in the binding table.

sip-mac - Filters traffic based on IP addresses and corresponding MAC addresses stored in the binding table.

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ Source guard is used to filter traffic on an insecure port which receives messages from outside the network or fire wall, and therefore may be subject to traffic attacks caused by a host trying to use the IP address of a neighbor.
- ◆ Setting source guard mode to "sip" or "sip-mac" enables this function on the selected port. Use the "sip" option to check the VLAN ID, source IP address, and port number against all entries in the binding table. Use the "sip-mac" option to check these same parameters, plus the source MAC address. Use the **no ip source guard** command to disable this function on the selected port.
- ◆ When enabled, traffic is filtered based upon dynamic entries learned via DHCP snooping, or static addresses configured in the source guard binding table.
- ◆ Table entries include a MAC address, IP address, lease time, entry type (Static-IP-SG-Binding, Dynamic-DHCP-Binding, VLAN identifier, and port identifier.

- ◆ Static addresses entered in the source guard binding table with the [ip source-guard binding](#) command are automatically configured with an infinite lease time. Dynamic entries learned via DHCP snooping are configured by the DHCP server itself.
- ◆ If the IP source guard is enabled, an inbound packet's IP address (sip option) or both its IP address and corresponding MAC address (sip-mac option) will be checked against the binding table. If no matching entry is found, the packet will be dropped.
- ◆ Filtering rules are implemented as follows:
 - If DHCPv4 snooping is disabled (see [page 301](#)), IP source guard will check the VLAN ID, source IP address, port number, and source MAC address (for the sip-mac option). If a matching entry is found in the binding table and the entry type is static IP source guard binding, the packet will be forwarded.
 - If the DHCP snooping is enabled, IP source guard will check the VLAN ID, source IP address, port number, and source MAC address (for the sip-mac option). If a matching entry is found in the binding table and the entry type is static IP source guard binding, or dynamic DHCP snooping binding, the packet will be forwarded.
 - If IP source guard is enabled on an interface for which IP source bindings (dynamically learned via DHCP snooping or manually configured) are not yet configured, the switch will drop all IP traffic on that port, except for DHCP packets.
 - Only unicast addresses are accepted for static bindings.

Example

This example enables IP source guard on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#ip source-guard sip
Console(config-if)#
```

Related Commands

[ip source-guard binding \(320\)](#)

[ip dhcp snooping \(301\)](#)

[ip dhcp snooping vlan \(306\)](#)

ip source-guard max-binding This command sets the maximum number of entries that can be bound to an interface. Use the **no** form to restore the default setting.

Syntax

ip source-guard max-binding *number*

no ip source-guard max-binding

number - The maximum number of IP addresses that can be mapped to an interface in the binding table. (Range: 1-5)

Default Setting

5

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ This command sets the maximum number of address entries that can be mapped to an interface in the binding table, including both dynamic entries discovered by DHCP snooping and static entries set by the **ip source-guard** command.

Example

This example sets the maximum number of allowed entries in the binding table for port 5 to one entry.

```
Console(config)#interface ethernet 1/5
Console(config-if)#ip source-guard max-binding 1
Console(config-if)#
```

show ip source-guard This command shows whether source guard is enabled or disabled on each interface.

Command Mode

Privileged Exec

Example

```
Console#show ip source-guard
Interface  Filter-type  Max-binding
-----
Eth 1/1    DISABLED          5
Eth 1/2    DISABLED          5
Eth 1/3    DISABLED          5
Eth 1/4    DISABLED          5
Eth 1/5    SIP               1
Eth 1/6    DISABLED          5
:
```

show ip source-guard binding This command shows the source guard binding table.

Syntax

show ip source-guard binding [dhcp-snooping | static]

dhcp-snooping - Shows dynamic entries configured with DHCP Snooping commands (see [page 300](#))

static - Shows static entries configured with the [ip source-guard binding](#) command (see [page 320](#)).

Command Mode

Privileged Exec

Example

```
Console#show ip source-guard binding
MAC Address      IP Address      Lease(sec)  Type           VLAN  Interface
-----
11-22-33-44-55-66 192.168.0.99      0 Static           1 Eth 1/5
Console#
```

IPv6 Source Guard

IPv6 Source Guard is a security feature that filters IPv6 traffic on non-routed, Layer 2 network interfaces based on manually configured entries in the IPv6 Source Guard table, or dynamic entries in the Neighbor Discovery Snooping table or DHCPv6 Snooping table when either snooping protocol is enabled (see [“DHCPv6 Snooping” on page 311](#)). IPv6 source guard can be used to prevent traffic attacks caused when a host tries to use the IPv6 address of a neighbor to access the network. This section describes commands used to configure IPv6 Source Guard.

Table 61: IPv6 Source Guard Commands

Command	Function	Mode
ipv6 source-guard binding	Adds a static address to the source-guard binding table	GC
ipv6 source-guard	Configures the switch to filter inbound traffic based on source IP address	IC
ipv6 source-guard max-binding	Sets the maximum number of entries that can be bound to an interface	IC
show ipv6 source-guard	Shows whether source guard is enabled or disabled on each interface	PE
show ipv6 source-guard binding	Shows the source guard binding table	PE

ipv6 source-guard binding This command adds a static address to the source-guard binding table. Use the **no** form to remove a static entry.

Syntax

ipv6 source-guard binding *mac-address* **vlan** *vlan-id* *ipv6-address*
interface ethernet *unit/port*

no ipv6 source-guard binding *mac-address* **vlan** *vlan-id*

mac-address - A valid unicast MAC address.

vlan-id - ID of a configured VLAN (Range: 1-4094)

ipv6-address - Corresponding IPv6 address. This address must be entered according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

Default Setting

No configured entries

Command Mode

Global Configuration

Command Usage

- ◆ Table entries include an associated MAC address, IPv6 global unicast address, lease time, entry type (Static-IP-SG-Binding, Dynamic-ND-Binding, Dynamic-DHCPv6-Binding), VLAN identifier, and port identifier.
- ◆ Traffic filtering is based only on the source IPv6 address, VLAN ID, and port number.
- ◆ All static entries are configured with an infinite lease time, which is indicated with a value of zero by the [show ipv6 source-guard](#) command.
- ◆ When source guard is enabled, traffic is filtered based upon dynamic entries learned via ND snooping, DHCPv6 snooping, or static addresses configured in the source guard binding table with this command.
- ◆ Static bindings are processed as follows:
 - If there is no entry with same and MAC address and IPv6 address, a new entry is added to binding table using static IP source guard binding.
 - If there is an entry with same MAC address and IPv6 address, and the type of entry is static IP source guard binding, then the new entry will replace the old one.

- If there is an entry with same MAC address and IPv6 address, and the type of the entry is either a dynamic ND snooping binding or DHCPv6 snooping binding, then the new entry will replace the old one and the entry type will be changed to static IP source guard binding.

Example

This example configures a static source-guard binding on port 5.

```
Console(config)#ipv6 source-guard binding 00-ab-11-cd-23-45 vlan 1 2001::1  
interface ethernet 1/5  
Console(config)#
```

Related Commands

[ipv6 source-guard \(326\)](#)

[ipv6 dhcp snooping \(312\)](#)

[ipv6 dhcp snooping vlan \(314\)](#)

ipv6 source-guard This command configures the switch to filter inbound traffic based on the source IP address stored in the binding table. Use the **no** form to disable this function.

Syntax

ipv6 source-guard sip

no ipv6 source-guard

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ Source guard is used to filter traffic on an insecure port which receives messages from outside the network or fire wall, and therefore may be subject to traffic attacks caused by a host trying to use the IP address of a neighbor.
- ◆ This command checks the VLAN ID, IPv6 global unicast source IP address, and port number against all entries in the binding table. Use the **no ipv6 source guard** command to disable this function on the selected port.
- ◆ After IPv6 source guard is enabled on an interface, the switch initially blocks all IPv6 traffic received on that interface, except for ND packets allowed by ND snooping and DHCPv6 packets allowed by DHCPv6 snooping. A port access control list (ACL) is applied to the interface. Traffic is then filtered based upon dynamic entries learned via ND snooping or DHCPv6 snooping, or static addresses configured in the source guard binding table. The port allows only

IPv6 traffic with a matching entry in the binding table and denies all other IPv6 traffic.

- ◆ Table entries include a MAC address, IPv6 global unicast address, lease time, entry type (Static-IP-SG-Binding, Dynamic-ND-Binding, Dynamic-DHCPv6-Binding), VLAN identifier, and port identifier.
- ◆ Static addresses entered in the source guard binding table with the [ipv6 source-guard binding](#) command are automatically configured with an infinite lease time. Dynamic entries learned via DHCPv6 snooping are configured by the DHCPv6 server itself.
- ◆ If IP source guard is enabled, an inbound packet's source IPv6 address will be checked against the binding table. If no matching entry is found, the packet will be dropped.
- ◆ Filtering rules are implemented as follows:
 - If ND snooping and DHCPv6 snooping are disabled, IP source guard will check the VLAN ID, source IPv6 address, and port number. If a matching entry is found in the binding table and the entry type is static IP source guard binding, the packet will be forwarded.
 - If ND snooping or DHCP snooping is enabled, IP source guard will check the VLAN ID, source IP address, and port number. If a matching entry is found in the binding table and the entry type is static IP source guard binding, dynamic ND snooping binding, or dynamic DHCPv6 snooping binding, the packet will be forwarded.
 - If IP source guard is enabled on an interface for which IPv6 source bindings (dynamically learned via ND snooping or DHCP snooping, or manually configured) are not yet configured, the switch will drop all IPv6 traffic on that port, except for ND packets and DHCPv6 packets.
 - Only IPv6 global unicast addresses are accepted for static bindings.

Example

This example enables IP source guard on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#ipv6 source-guard sip
Console(config-if)#
```

Related Commands

[ipv6 source-guard binding \(325\)](#)

[ipv6 dhcp snooping \(312\)](#)

[ipv6 dhcp snooping vlan \(314\)](#)

ipv6 source-guard max-binding This command sets the maximum number of entries that can be bound to an interface. Use the **no** form to restore the default setting.

Syntax

ipv6 source-guard max-binding *number*

no ipv6 source-guard max-binding

number - The maximum number of IPv6 addresses that can be mapped to an interface in the binding table. (Range: 1-5)

Default Setting

5

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ This command sets the maximum number of address entries that can be mapped to an interface in the binding table, including both dynamic entries discovered by ND snooping, DHCPv6 snooping, and static entries set by the **ipv6 source-guard** command.
- ◆ IPv6 source guard maximum bindings must be set to a value higher than DHCPv6 snooping maximum bindings and ND snooping maximum bindings.
- ◆ If IPv6 source guard, ND snooping, and DHCPv6 snooping are enabled on a port, the dynamic bindings used by ND snooping, DHCPv6 snooping, and IPv6 source guard static bindings cannot exceed the maximum allowed bindings set by the **ipv6 source-guard max-binding** command. In other words, no new entries will be added to the IPv6 source guard binding table.
- ◆ If IPv6 source guard is enabled on a port, and the maximum number of allowed bindings is changed to a lower value, precedence is given to deleting entries learned through DHCPv6 snooping, ND snooping, and then manually configured IPv6 source guard static bindings, until the number of entries in the binding table reaches the newly configured maximum number of allowed bindings.

Example

This example sets the maximum number of allowed entries in the binding table for port 5 to one entry.

```
Console(config)#interface ethernet 1/5
Console(config-if)#ipv6 source-guard max-binding 1
Console(config-if)#
```


show ipv6 source-guard This command shows whether IPv6 source guard is enabled or disabled on each interface, and the maximum allowed bindings.

Command Mode

Privileged Exec

Example

```
Console#show ipv6 source-guard
Interface  Filter-type  Max-binding
-----
Eth 1/1    DISABLED      5
Eth 1/2    DISABLED      5
Eth 1/3    DISABLED      5
Eth 1/4    DISABLED      5
Eth 1/5    SIP           1
Eth 1/6    DISABLED      5
:
```

show ipv6 source-guard binding This command shows the source guard binding table.

Syntax

show ipv6 source-guard binding [dynamic | static]

dynamic - Shows dynamic entries configured with ND Snooping or DHCPv6 Snooping commands (see [page 311](#))

static - Shows static entries configured with the [ipv6 source-guard binding](#) command.

Command Mode

Privileged Exec

Example

```
Console#show ipv6 source-guard binding
MAC Address  IPv6 Address  VLAN Interface Type
-----
00AB-11CD-2345  2001::1      1  Eth 1/5  STA
Console#
```

ARP Inspection

ARP Inspection validates the MAC-to-IP address bindings in Address Resolution Protocol (ARP) packets. It protects against ARP traffic with invalid address bindings, which forms the basis for certain “man-in-the-middle” attacks. This is accomplished by intercepting all ARP requests and responses and verifying each of these packets before the local ARP cache is updated or the packet is forwarded to the appropriate destination, dropping any invalid ARP packets.

ARP Inspection determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database – the DHCP snooping binding database. ARP Inspection can also validate ARP packets against user-configured ARP access control lists (ACLs) for hosts with statically configured IP addresses.

This section describes commands used to configure ARP Inspection.

Table 62: ARP Inspection Commands

Command	Function	Mode
<code>ip arp inspection</code>	Enables ARP Inspection globally on the switch	GC
<code>ip arp inspection filter</code>	Specifies an ARP ACL to apply to one or more VLANs	GC
<code>ip arp inspection log-buffer logs</code>	Sets the maximum number of entries saved in a log message, and the rate at these messages are sent	GC
<code>ip arp inspection validate</code>	Specifies additional validation of address components in an ARP packet	GC
<code>ip arp inspection vlan</code>	Enables ARP Inspection for a specified VLAN or range of VLANs	GC
<code>ip arp inspection limit</code>	Sets a rate limit for the ARP packets received on a port	IC
<code>ip arp inspection trust</code>	Sets a port as trusted, and thus exempted from ARP Inspection	IC
<code>show ip arp inspection configuration</code>	Displays the global configuration settings for ARP Inspection	PE
<code>show ip arp inspection interface</code>	Shows the trust status and inspection rate limit for ports	PE
<code>show ip arp inspection log</code>	Shows information about entries stored in the log, including the associated VLAN, port, and address components	PE
<code>show ip arp inspection statistics</code>	Shows statistics about the number of ARP packets processed, or dropped for various reasons	PE
<code>show ip arp inspection vlan</code>	Shows configuration setting for VLANs, including ARP Inspection status, the ARP ACL name, and if the DHCP Snooping database is used after ACL validation is completed	PE

ip arp inspection This command enables ARP Inspection globally on the switch. Use the **no** form to disable this function.

Syntax

[no] ip arp inspection

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ When ARP Inspection is enabled globally with this command, it becomes active only on those VLANs where it has been enabled with the **ip arp inspection vlan** command.
- ◆ When ARP Inspection is enabled globally and enabled on selected VLANs, all ARP request and reply packets on those VLANs are redirected to the CPU and their switching is handled by the ARP Inspection engine.
- ◆ When ARP Inspection is disabled globally, it becomes inactive for all VLANs, including those where ARP Inspection is enabled.
- ◆ When ARP Inspection is disabled, all ARP request and reply packets bypass the ARP Inspection engine and their manner of switching matches that of all other packets.
- ◆ Disabling and then re-enabling global ARP Inspection will not affect the ARP Inspection configuration for any VLANs.
- ◆ When ARP Inspection is disabled globally, it is still possible to configure ARP Inspection for individual VLANs. These configuration changes will only become active after ARP Inspection is globally enabled again.

Example

```
Console(config)#ip arp inspection
Console(config)#
```

ip arp inspection filter This command specifies an ARP ACL to apply to one or more VLANs. Use the **no** form to remove an ACL binding.

Syntax

ip arp inspection filter *arp-acl-name* **vlan** {*vlan-id* | *vlan-range*} [**static**]

arp-acl-name - Name of an ARP ACL. (Maximum length: 16 characters)

vlan-id - VLAN ID. (Range: 1-4094)

vlan-range - A consecutive range of VLANs indicated by the use a hyphen, or a random group of VLANs with each entry separated by a comma.

static - ARP packets are only validated against the specified ACL, address bindings in the DHCP snooping database is not checked.

Default Setting

ARP ACLs are not bound to any VLAN
Static mode is not enabled

Command Mode

Global Configuration

Command Usage

- ◆ ARP ACLs are configured with the commands described on [“ARP ACLs” on page 364](#).
- ◆ If static mode is enabled, the switch compares ARP packets to the specified ARP ACLs. Packets matching an IP-to-MAC address binding in a permit or deny rule are processed accordingly. Packets not matching any of the ACL rules are dropped. Address bindings in the DHCP snooping database are not checked.
- ◆ If static mode is not enabled, packets are first validated against the specified ARP ACL. Packets matching a deny rule are dropped. All remaining packets are validated against the address bindings in the DHCP snooping database.

Example

```
Console(config)#ip arp inspection filter sales vlan 1
Console(config)#
```

ip arp inspection log-buffer logs This command sets the maximum number of entries saved in a log message, and the rate at which these messages are sent. Use the **no** form to restore the default settings.

Syntax

ip arp inspection log-buffer logs *message-number* **interval** *seconds*

no ip arp inspection log-buffer logs

message-number - The maximum number of entries saved in a log message.
(Range: 0-256, where 0 means no events are saved)

seconds - The interval at which log messages are sent. (Range: 0-86400)

Default Setting

Message Number: 5

Interval: 1 second

Command Mode

Global Configuration

Command Usage

- ◆ ARP Inspection must be enabled with the **ip arp inspection** command before this command will be accepted by the switch.
- ◆ By default, logging is active for ARP Inspection, and cannot be disabled.
- ◆ When the switch drops a packet, it places an entry in the log buffer. Each entry contains flow information, such as the receiving VLAN, the port number, the source and destination IP addresses, and the source and destination MAC addresses.
- ◆ If multiple, identical invalid ARP packets are received consecutively on the same VLAN, then the logging facility will only generate one entry in the log buffer and one corresponding system message.
- ◆ The maximum number of entries that can be stored in the log buffer is determined by the *message-number* parameter. If the log buffer fills up before a message is sent, the oldest entry will be replaced with the newest one.
- ◆ The switch generates a system message on a rate-controlled basis determined by the *seconds* values. After the system message is generated, all entries are cleared from the log buffer.

Example

```
Console(config)#ip arp inspection log-buffer logs 1 interval 10
Console(config)#
```

ip arp inspection validate This command specifies additional validation of address components in an ARP packet. Use the **no** form to restore the default setting.

Syntax

ip arp inspection validate {**dst-mac** [**ip**] [**src-mac**] |
ip [**src-mac**] | **src-mac**}

no ip arp inspection validate

dst-mac - Checks the destination MAC address in the Ethernet header against the target MAC address in the ARP body. This check is performed for ARP responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

ip - Checks the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. Sender IP addresses are checked in all ARP requests and responses, while target IP addresses are checked only in ARP responses.

src-mac - Checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

Default Setting

No additional validation is performed

Command Mode

Global Configuration

Command Usage

By default, ARP Inspection only checks the IP-to-MAC address bindings specified in an ARP ACL or in the DHCP Snooping database.

Example

```
Console(config)#ip arp inspection validate dst-mac
Console(config)#
```

ip arp inspection vlan This command enables ARP Inspection for a specified VLAN or range of VLANs. Use the **no** form to disable this function.

Syntax

[no] ip arp inspection vlan {**vlan-id** | **vlan-range**}

vlan-id - VLAN ID. (Range: 1-4094)

vlan-range - A consecutive range of VLANs indicated by the use a hyphen, or a random group of VLANs with each entry separated by a comma.

Default Setting

Disabled on all VLANs

Command Mode

Global Configuration

Command Usage

- ◆ When ARP Inspection is enabled globally with the `ip arp inspection` command, it becomes active only on those VLANs where it has been enabled with this command.
- ◆ When ARP Inspection is enabled globally and enabled on selected VLANs, all ARP request and reply packets on those VLANs are redirected to the CPU and their switching is handled by the ARP Inspection engine.
- ◆ When ARP Inspection is disabled globally, it becomes inactive for all VLANs, including those where ARP Inspection is enabled.
- ◆ When ARP Inspection is disabled, all ARP request and reply packets bypass the ARP Inspection engine and their manner of switching matches that of all other packets.
- ◆ Disabling and then re-enabling global ARP Inspection will not affect the ARP Inspection configuration for any VLANs.
- ◆ When ARP Inspection is disabled globally, it is still possible to configure ARP Inspection for individual VLANs. These configuration changes will only become active after ARP Inspection is globally enabled again.

Example

```
Console(config)#ip arp inspection vlan 1,2
Console(config)#
```

ip arp inspection limit This command sets a rate limit for the ARP packets received on a port. Use the **no** form to restore the default setting.

Syntax

ip arp inspection limit {rate *pps* | none}

no ip arp inspection limit

pps - The maximum number of ARP packets that can be processed by the CPU per second. (Range: 0-2048, where 0 means that no ARP packets can be forwarded)

none - There is no limit on the number of ARP packets that can be processed by the CPU.

Default Setting

15

Command Mode

Interface Configuration (Port, Static Aggregation)

Command Usage

- ◆ This command only applies to untrusted ports.
- ◆ When the rate of incoming ARP packets exceeds the configured limit, the switch drops all ARP packets in excess of the limit.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip arp inspection limit rate 150
Console(config-if)#
```

ip arp inspection trust This command sets a port as trusted, and thus exempted from ARP Inspection. Use the **no** form to restore the default setting.

Syntax

[no] ip arp inspection trust

Default Setting

Untrusted

Command Mode

Interface Configuration (Port, Static Aggregation)

Command Usage

Packets arriving on untrusted ports are subject to any configured ARP Inspection and additional validation checks. Packets arriving on trusted ports bypass all of these checks, and are forwarded according to normal switching rules.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip arp inspection trust
Console(config-if)#
```


show ip arp inspection configuration This command displays the global configuration settings for ARP Inspection.

Command Mode
Privileged Exec

Example

```
Console#show ip arp inspection configuration

ARP Inspection Global Information:

Global IP ARP Inspection Status : disabled
Log Message Interval           : 10 s
Log Message Number              : 1
Need Additional Validation(s)   : Yes
Additional Validation Type       : Destination MAC address
Console#
```

show ip arp inspection interface This command shows the trust status and ARP Inspection rate limit for ports.

Syntax

show ip arp inspection interface [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

Command Mode
Privileged Exec

Example

```
Console#show ip arp inspection interface ethernet 1/1

Port Number      Trust Status      Limit Rate (pps)
-----
Eth 1/1          Trusted           150
Console#
```

show ip arp inspection log This command shows information about entries stored in the log, including the associated VLAN, port, and address components.

Command Mode
Privileged Exec

Example

```
Console#show ip arp inspection log
Total log entries number is 1

Num VLAN Port Src IP Address Dst IP Address Src MAC Address Dst MAC Address
--- --
1 1 11 192.168.2.2 192.168.2.1 00-04-E2-A0-E2-7C FF-FF-FF-FF-FF-FF
Console#
```

show ip arp inspection statistics This command shows statistics about the number of ARP packets processed, or dropped for various reasons.

Command Mode
Privileged Exec

Example

```
Console#show ip arp inspection statistics

ARP packets received before rate limit : 150
ARP packets dropped due to rate limit : 5
Total ARP packets processed by ARP Inspection : 150
ARP packets dropped by additional validation (source MAC address) : 0
ARP packets dropped by additional validation (destination MAC address): 0
ARP packets dropped by additional validation (IP address) : 0
ARP packets dropped by ARP ACLs : 0
ARP packets dropped by DHCP snooping : 0

Console#
```

show ip arp inspection vlan This command shows the configuration settings for VLANs, including ARP Inspection status, the ARP ACL name, and if the DHCP Snooping database is used after ARP ACL validation is completed.

Syntax

show ip arp inspection vlan [*vlan-id* | *vlan-range*]

vlan-id - VLAN ID. (Range: 1-4094)

vlan-range - A consecutive range of VLANs indicated by the use a hyphen, or a random group of VLANs with each entry separated by a comma.

Command Mode
Privileged Exec

Example

```
Console#show ip arp inspection vlan 1
```

VLAN ID	DAI Status	ACL Name	ACL Status
1	disabled	sales	static

```
Console#
```

Denial of Service Protection

A denial-of-service attack (DoS attack) is an attempt to block the services provided by a computer or network resource. This kind of attack tries to prevent an Internet site or service from functioning efficiently or at all. In general, DoS attacks are implemented by either forcing the target to reset, to consume most of its resources so that it can no longer provide its intended service, or to obstruct the communication media between the intended users and the target so that they can no longer communicate adequately.

This section describes commands used to protect against DoS attacks.

Table 63: DoS Protection Commands

Command	Function	Mode
<code>dos-protection land</code>	Protects against DoS LAND attacks	GC
<code>dos-protection tcp-null-scan</code>	Protects against DoS TCP-null-scan attacks	GC
<code>dos-protection tcp-syn-fin-scan</code>	Protects against DoS TCP-SYN/FIN-scan attacks	GC
<code>dos-protection tcp-xmas-scan</code>	Protects against DoS TCP-XMAS-scan attacks	GC
<code>show dos-protection</code>	Shows the configuration settings for DoS protection	PE

dos-protection land This command protects against DoS LAND (Local Area Network Denial) attacks in which hackers send spoofed-IP packets where the source and destination address are the same, thereby causing the target to reply to itself continuously. Use the **no** form to disable this feature.

Syntax

[no] dos-protection land

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#dos-protection land
Console(config)#
```

dos-protection tcp-null-scan

This command protects against TCP-null-scan attacks in which a TCP NULL scan message is used to identify listening TCP ports. The scan uses a series of strangely configured TCP packets which contain a sequence number of 0 and no flags. If the target's TCP port is closed, the target replies with a TCP RST (reset) packet. If the target TCP port is open, it simply discards the TCP NULL scan. Use the **no** form to disable this feature.

Syntax

[no] dos-protection tcp-null-scan

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

In these packets, all TCP flags are 0.

Example

```
Console(config)#dos-protection tcp-null-scan
Console(config)#
```

dos-protection tcp-syn-fin-scan

This command protects against DoS TCP-SYN/FIN-scan attacks in which a TCP SYN/FIN scan message is used to identify listening TCP ports. The scan uses a series of strangely configured TCP packets which contain SYN (synchronize) and FIN (finish) flags. If the target's TCP port is closed, the target replies with a TCP RST (reset) packet. If the target TCP port is open, it simply discards the TCP SYN FIN scan. Use the **no** form to disable this feature.

Syntax

[no] dos-protection syn-fin-scan

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

In these packets, SYN=1 and FIN=1.

Example

```
Console(config)#dos-protection syn-fin-scan
Console(config)#
```

dos-protection tcp-xmas-scan

This command protects against TCP-xmas-scan in which a so-called TCP XMAS scan message is used to identify listening TCP ports. This scan uses a series of strangely configured TCP packets which contain a sequence number of 0 and the URG, PSH and FIN flags. If the target's TCP port is closed, the target replies with a TCP RST packet. If the target TCP port is open, it simply discards the TCP XMAS scan. Use the **no** form to disable this feature.

Syntax

[no] dos-protection tcp-xmas-scan

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

In these packets, FIN=1, URG= 1 and PSH = 1.

Example

```
Console(config)#dos-protection tcp-xmas-scan
Console(config)#
```

show dos-protection This command shows the configuration settings for the DoS protection commands.

Command Mode

Privileged Exec

Example

```
Console#show dos-protection
Global DoS Protections:

LAND Attack           : Enabled
TCP Null Scan         : Enabled
TCP SYN/FIN Scan      : Enabled
TCP XMAS Scan         : Enabled
Console#
```

Port-based Traffic Segmentation

If tighter security is required for passing traffic from different clients through downlink ports on the local network and over uplink ports to the service provider, port-based traffic segmentation can be used to isolate traffic for individual clients.

Traffic belonging to each client is isolated to the allocated downlink ports. But the switch can be configured to either isolate traffic passing across a client's allocated uplink ports from the uplink ports assigned to other clients, or to forward traffic through the uplink ports used by other clients, allowing different clients to share access to their uplink ports where security is less likely to be compromised.

Table 64: Commands for Configuring Traffic Segmentation

Command	Function	Mode
<code>traffic-segmentation</code>	Enables traffic segmentation	GC
<code>traffic-segmentation session</code>	Creates a client session	GC
<code>traffic-segmentation uplink/ downlink</code>	Configures uplink/downlink ports for client sessions	GC
<code>traffic-segmentation uplink-to- uplink</code>	Specifies whether or not traffic can be forwarded between uplink ports assigned to different client sessions	GC
<code>show traffic-segmentation</code>	Displays the configured traffic segments	PE

traffic-segmentation This command enables traffic segmentation. Use the **no** form to disable traffic segmentation.

Syntax

[no] traffic-segmentation

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ Traffic segmentation provides port-based security and isolation between ports within the VLAN. Data traffic on the downlink ports can only be forwarded to, and from, the designated uplink port(s). Data cannot pass between downlink ports in the same segmented group, nor to ports which do not belong to the same group.
- ◆ Traffic segmentation and normal VLANs can exist simultaneously within the same switch. Traffic may pass freely between uplink ports in segmented groups and ports in normal VLANs.

- ◆ When traffic segmentation is enabled, the forwarding state for the uplink and downlink ports assigned to different client sessions is shown below.

Table 65: Traffic Segmentation Forwarding

Destination Source	Session #1 Downlinks	Session #1 Uplinks	Session #2 Downlinks	Session #2 Uplinks	Normal Ports
Session #1 Downlink Ports	Blocking	Forwarding	Blocking	Blocking	Blocking
Session #1 Uplink Ports	Forwarding	Forwarding	Blocking	Blocking/Forwarding*	Forwarding
Session #2 Downlink Ports	Blocking	Blocking	Blocking	Forwarding	Blocking
Session #2 Uplink Ports	Blocking	Blocking/Forwarding<Superscript>*	Forwarding	Forwarding	Forwarding
Normal Ports	Forwarding	Forwarding	Forwarding	Forwarding	Forwarding

* The forwarding state for uplink-to-uplink ports is configured by the [traffic-segmentation uplink-to-uplink](#) command.

- ◆ When traffic segmentation is disabled, all ports operate in normal forwarding mode based on the settings specified by other functions such as VLANs and spanning tree protocol.
- ◆ Enter the **traffic-segmentation** command without any parameters to enable traffic segmentation. Then set the interface members for segmented groups using the [traffic-segmentation uplink/downlink](#) command.
- ◆ Enter **no traffic-segmentation** to disable traffic segmentation and clear the configuration settings for segmented groups.

Example

This example enables traffic segmentation globally on the switch.

```
Console(config)#traffic-segmentation
Console(config)#
```

traffic-segmentation session This command creates a traffic-segmentation client session. Use the **no** form to remove a client session.

Syntax

[no] pvlan session session-id

session-id – Traffic segmentation session. (Range: 1-4)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ Use this command to create a new traffic-segmentation client session.
- ◆ Using the **no** form of this command will remove any assigned uplink or downlink ports, restoring these interfaces to normal operating mode.

Example

```
Console(config)#traffic-segmentation session 1
Console(config)#
```

traffic-segmentation uplink/downlink This command configures the uplink and down-link ports for a segmented group of ports. Use the **no** form to remove a port from the segmented group.

Syntax

[no] traffic-segmentation [session session-id] {uplink interface-list [downlink interface-list] | downlink interface-list}

session-id – Traffic segmentation session. (Range: 1-4)

uplink – Specifies an uplink interface.

downlink – Specifies a downlink interface.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Default Setting

Session 1 if not defined

No segmented port groups are defined.

Command Mode

Global Configuration

Command Usage

- ◆ A port cannot be configured in both an uplink and downlink list.
- ◆ A port can only be assigned to one traffic-segmentation session.
- ◆ When specifying an uplink or downlink, a list of ports may be entered by using a hyphen or comma in the *port* field. Note that lists are not supported for the *channel-id* field.

- ◆ A downlink port can only communicate with an uplink port in the same session. Therefore, if an uplink port is not configured for a session, the assigned downlink ports will not be able to communicate with any other ports.
- ◆ If a downlink port is not configured for the session, the assigned uplink ports will operate as normal ports.

Example

This example enables traffic segmentation, and then sets port 10 as the uplink and ports 5-8 as downlinks.

```
Console(config)#traffic-segmentation
Console(config)#traffic-segmentation uplink ethernet 1/10
downlink ethernet 1/5-8
Console(config)#
```

traffic-segmentation uplink-to-uplink This command specifies whether or not traffic can be forwarded between uplink ports assigned to different client sessions. Use the **no** form to restore the default.

Syntax

[no] traffic-segmentation uplink-to-uplink {blocking | forwarding}

blocking – Blocks traffic between uplink ports assigned to different sessions.

forwarding – Forwards traffic between uplink ports assigned to different sessions.

Default Setting

Blocking

Command Mode

Global Configuration

Example

This example enables forwarding of traffic between uplink ports assigned to different client sessions.

```
Console(config)#traffic-segmentation uplink-to-uplink forwarding
Console(config)#
```

show traffic-segmentation This command displays the configured traffic segments.

Command Mode
Privileged Exec

Example

```
Console#show traffic-segmentation
```

```
Private VLAN Status      : Enabled
Uplink-to-Uplink Mode    : Forwarding
```

Session	Uplink Ports	Downlink Ports
1	Ethernet 1/1	Ethernet 1/2 Ethernet 1/3 Ethernet 1/4

```
Console#
```

Access Control Lists

Access Control Lists (ACL) provide packet filtering for IPv4 frames (based on address, protocol, Layer 4 protocol port number or TCP control code), IPv6 frames (based on address, DSCP traffic class, next header type, or flow label), or any frames (based on MAC address or Ethernet type). To filter packets, first create an access list, add the required rules, and then bind the list to a specific port. This section describes the Access Control List commands.

Table 66: Access Control List Commands

Command Group	Function
IPv4 ACLs	Configures ACLs based on IPv4 addresses, TCP/UDP port number, protocol type, and TCP control code
IPv6 ACLs	Configures ACLs based on IPv6 addresses, DSCP traffic class, next header type, or flow label
MAC ACLs	Configures ACLs based on hardware addresses, packet format, and Ethernet type
ARP ACLs	Configures ACLs based on ARP messages addresses
ACL Information	Displays ACLs and associated rules; shows ACLs assigned to each port

IPv4 ACLs

The commands in this section configure ACLs based on IPv4 addresses, TCP/UDP port number, protocol type, and TCP control code. To configure IPv4 ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more ports.

Table 67: IPv4 ACL Commands

Command	Function	Mode
access-list ip	Creates an IP ACL and enters configuration mode for standard or extended IPv4 ACLs	GC
permit, deny	Filters packets matching a specified source IPv4 address	IPv4-STD-ACL
permit, deny	Filters packets meeting the specified criteria, including source and destination IPv4 address, TCP/UDP port number, protocol type, and TCP control code	IPv4-EXT-ACL
ip access-group	Binds an IPv4 ACL to a port	IC
show ip access-group	Shows port assignments for IPv4 ACLs	PE
show ip access-list	Displays the rules for configured IPv4 ACLs	PE

access-list ip This command adds an IP access list and enters configuration mode for standard or extended IPv4 ACLs. Use the **no** form to remove the specified ACL.

Syntax

[no] access-list ip {standard | extended} *acl-name*

standard – Specifies an ACL that filters packets based on the source IP address.

extended – Specifies an ACL that filters packets based on the source or destination IP address, and other more specific criteria.

acl-name – Name of the ACL. (Maximum length: 32 characters, no spaces or other special characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list.
- ◆ To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- ◆ An ACL can contain up to 96 rules.

Example

```
Console(config)#access-list ip standard david
Console(config-std-acl)#
```

Related Commands

[permit, deny \(349\)](#)

[ip access-group \(352\)](#)

[show ip access-list \(353\)](#)

permit, deny (Standard IP ACL) This command adds a rule to a Standard IPv4 ACL. The rule sets a filter condition for packets emanating from the specified source. Use the **no** form to remove a rule.

Syntax

```
{permit | deny} {any | source bitmask | host source}  
[time-range time-range-name]  
no {permit | deny} {any | source bitmask | host source}
```

any – Any source IP address.

source – Source IP address.

bitmask – Dotted decimal number representing the address bits to match.

host – Keyword followed by a specific IP address.

time-range-name - Name of the time range. (Range: 1-30 characters)

Default Setting

None

Command Mode

Standard IPv4 ACL

Command Usage

- ◆ New rules are appended to the end of the list.
- ◆ Address bit masks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bits to indicate “match” and 0 bits to indicate “ignore.” The bitmask is bitwise ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.

Example

This example configures one permit rule for the specific address 10.1.1.21 and another rule for the address range 168.92.16.x – 168.92.31.x using a bitmask.

```
Console(config-std-acl)#permit host 10.1.1.21  
Console(config-std-acl)#permit 168.92.16.0 255.255.240.0  
Console(config-std-acl)#
```

Related Commands

[access-list ip \(348\)](#)

[Time Range \(169\)](#)

permit, deny (Extended IPv4 ACL) This command adds a rule to an Extended IPv4 ACL. The rule sets a filter condition for packets with specific source or destination IP addresses, protocol types, source or destination protocol ports, or TCP control codes. Use the **no** form to remove a rule.

Syntax

```
{permit | deny} [protocol-number | udp]  
  {any | source address-bitmask | host source}  
  {any | destination address-bitmask | host destination}  
  [precedence precedence] [tos tos] [dscp dscp]  
  [source-port sport [bitmask]]  
  [destination-port dport [port-bitmask]]  
  [time-range time-range-name]
```

```
no {permit | deny} [protocol-number | udp]  
  {any | source address-bitmask | host source}  
  {any | destination address-bitmask | host destination}  
  [precedence precedence] [tos tos] [dscp dscp]  
  [source-port sport [bitmask]]  
  [destination-port dport [port-bitmask]]
```

```
{permit | deny} tcp  
  {any | source address-bitmask | host source}  
  {any | destination address-bitmask | host destination}  
  [precedence precedence] [tos tos] [dscp dscp]  
  [source-port sport [bitmask]]  
  [destination-port dport [port-bitmask]]  
  [control-flag control-flags flag-bitmask]  
  [time-range time-range-name]
```

```
no {permit | deny} tcp  
  {any | source address-bitmask | host source}  
  {any | destination address-bitmask | host destination}  
  [precedence precedence] [tos tos] [dscp dscp]  
  [source-port sport [bitmask]]  
  [destination-port dport [port-bitmask]]  
  [control-flag control-flags flag-bitmask]
```

protocol-number – A specific protocol number. (Range: 0-255)

source – Source IP address.

destination – Destination IP address.

address-bitmask – Decimal number representing the address bits to match.

host – Keyword followed by a specific IP address.

precedence – IP precedence level. (Range: 0-7)

tos – Type of Service level. (Range: 0-15)

dscp – DSCP priority level. (Range: 0-63)

sport – Protocol⁴ source port number. (Range: 0-65535)

4. Includes TCP, UDP or other protocol types.

dport – Protocol⁴ destination port number. (Range: 0-65535)

port-bitmask – Decimal number representing the port bits to match. (Range: 0-65535)

control-flags – Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)

flag-bitmask – Decimal number representing the code bits to match.

time-range-name - Name of the time range. (Range: 1-30 characters)

Default Setting

None

Command Mode

Extended IPv4 ACL

Command Usage

- ◆ All new rules are appended to the end of the list.
- ◆ Address bit masks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bits to indicate “match” and 0 bits to indicate “ignore.” The bit mask is bitwise ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.
- ◆ You can specify both Precedence and ToS in the same rule. However, if DSCP is used, then neither Precedence nor ToS can be specified.
- ◆ The control-code bitmask is a decimal number (representing an equivalent bit mask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit “1” means to match a bit and “0” means to ignore a bit. The following bits may be specified:
 - 1 (fin) – Finish
 - 2 (syn) – Synchronize
 - 4 (rst) – Reset
 - 8 (psh) – Push
 - 16 (ack) – Acknowledgement
 - 32 (urg) – Urgent pointer

For example, use the code value and mask below to catch packets with the following flags set:

- SYN flag valid, use “control-code 2 2”
- Both SYN and ACK valid, use “control-code 18 18”
- SYN valid and ACK invalid, use “control-code 2 18”

Example

This example accepts any incoming packets if the source address is within subnet 10.7.1.x. For example, if the rule is matched; i.e., the rule (10.7.1.0 & 255.255.255.0) equals the masked address (10.7.1.2 & 255.255.255.0), the packet passes through.

```
Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any
Console(config-ext-acl)#
```

This allows TCP packets from class C addresses 192.168.1.0 to any destination address when set for destination TCP port 80 (i.e., HTTP).

```
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any destination-port
80
Console(config-ext-acl)#
```

This permits all TCP packets from class C addresses 192.168.1.0 with the TCP control code set to "SYN."

```
Console(config-ext-acl)#permit tcp 192.168.1.0 255.255.255.0 any control-
flag 2 2
Console(config-ext-acl)#
```

Related Commands

[access-list ip \(348\)](#)

[Time Range \(169\)](#)

ip access-group This command binds an IPv4 ACL to a port. Use the **no** form to remove the port.

Syntax

ip access-group *acl-name* **in** [**time-range** *time-range-name*]

no ip access-group *acl-name* **in**

acl-name – Name of the ACL. (Maximum length: 16 characters)

in – Indicates that this list applies to ingress packets.

time-range-name - Name of the time range. (Range: 1-30 characters)

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

◆ Only one ACL can be bound to a port.

- ◆ If an ACL is already bound to a port and you bind a different ACL to it, the switch will replace the old binding with the new one.

Example

```
Console(config)#int eth 1/2
Console(config-if)#ip access-group david in
Console(config-if)#
```

Related Commands

[show ip access-list \(353\)](#)

[Time Range \(169\)](#)

show ip access-group This command shows the ports assigned to IP ACLs.

Command Mode

Privileged Exec

Example

```
Console#show ip access-group
Interface ethernet 1/2
IP access-list david in
Console#
```

Related Commands

[ip access-group \(352\)](#)

show ip access-list This command displays the rules for configured IPv4 ACLs.

Syntax

show ip access-list {standard | extended} [acl-name]

standard – Specifies a standard IP ACL.

extended – Specifies an extended IP ACL.

acl-name – Name of the ACL. (Maximum length: 16 characters)

Command Mode

Privileged Exec

Example

```
Console#show ip access-list standard
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.0.0 255.255.15.0
Console#
```

Related Commands
[permit, deny \(349\)](#)
[ip access-group \(352\)](#)

IPv6 ACLs

The commands in this section configure ACLs based on IPv6 address, DSCP traffic class, next header type, or flow label. To configure IPv6 ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more ports.

Table 68: IPv6 ACL Commands

Command	Function	Mode
access-list ipv6	Creates an IPv6 ACL and enters configuration mode for standard or extended IPv6 ACLs	GC
permit, deny	Filters packets matching a specified source IPv6 address	IPv6- STD-ACL
permit, deny	Filters packets meeting a specified criteria, including destination IPv6 address	IPv6- EXT-ACL
show ipv6 access-list	Displays the rules for configured IPv6 ACLs	PE
ipv6 access-group	Adds a port to an IPv6 ACL	IC
show ipv6 access-group	Shows port assignments for IPv6 ACLs	PE

access-list ipv6 This command adds an IP access list and enters configuration mode for standard or extended IPv6 ACLs. Use the **no** form to remove the specified ACL.

Syntax

[no] access-list ipv6 {standard | extended} *acl-name*

standard – Specifies an ACL that filters packets based on the source IP address.

extended – Specifies an ACL that filters packets based on the destination IP address, and other more specific criteria.

acl-name – Name of the ACL. (Maximum length: 32 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list. To create an ACL, you must add at least one rule to the list.
- ◆ To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- ◆ An ACL can contain up to 96 rules.

Example

```
Console(config)#access-list ipv6 standard david
Console(config-std-ipv6-acl)#
```

Related Commands

[permit, deny \(Standard IPv6 ACL\) \(355\)](#)
[permit, deny \(Extended IPv6 ACL\) \(356\)](#)
[ipv6 access-group \(358\)](#)
[show ipv6 access-list \(357\)](#)

permit, deny (Standard IPv6 ACL) This command adds a rule to a Standard IPv6 ACL. The rule sets a filter condition for packets emanating from the specified source. Use the **no** form to remove a rule.

Syntax

```
{permit | deny} {any | host source-ipv6-address |  

source-ipv6-address[/prefix-length]}  

[time-range time-range-name]
```

```
no {permit | deny} {any | host source-ipv6-address |  

source-ipv6-address[/prefix-length]}
```

any – Any source IP address.

host – Keyword followed by a specific IP address.

source-ipv6-address - An IPv6 source address or network class. The address must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

prefix-length - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix; i.e., the network portion of the address. (Range: 0-128)

time-range-name - Name of the time range. (Range: 1-16 characters)

Default Setting

None

Command Mode

Standard IPv6 ACL

Command Usage

New rules are appended to the end of the list.

Example

This example configures one permit rule for the specific address 2009:DB9:2229::79 and another rule for the addresses with the network prefix 2009:DB9:2229:5::/64.

```
Console(config-std-ipv6-acl)#permit host 2009:DB9:2229::79
Console(config-std-ipv6-acl)#permit 2009:DB9:2229:5::/64
Console(config-std-ipv6-acl)#
```

Related Commands

[access-list ipv6 \(354\)](#)

[Time Range \(169\)](#)

permit, deny (Extended IPv6 ACL)

This command adds a rule to an Extended IPv6 ACL. The rule sets a filter condition for packets with specific destination IP addresses, next header type, or flow label. Use the **no** form to remove a rule.

Syntax

{permit | deny} {any | host destination-ipv6-address | destination-ipv6-address[/prefix-length]} [time-range time-range-name]

no {permit | deny} {any | host destination-ipv6-address | destination-ipv6-address[/prefix-length]}

any – Any IP address (an abbreviation for the IPv6 prefix ::/0).

host – Keyword followed by a specific destination IP address.

destination-ipv6-address - An IPv6 destination address or network class. The address must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

prefix-length - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix; i.e., the network portion of the address. (Range: 0-64)

time-range-name - Name of the time range.
(Range: 1-30 characters)

Default Setting

None

Command Mode

Extended IPv6 ACL

Command Usage

- ◆ All new rules are appended to the end of the list.

Example

This example accepts any incoming packets if the destination address is 2009:DB9:2229::79/8.

```
Console(config-ext-ipv6-acl)#permit 2009:DB9:2229::79/8
Console(config-ext-ipv6-acl)#
```

Related Commands

[access-list ipv6 \(354\)](#)

[Time Range \(169\)](#)

show ipv6 access-list This command displays the rules for configured IPv6 ACLs.

Syntax

show ipv6 access-list {**standard** | **extended**} [*acl-name*]

standard – Specifies a standard IPv6 ACL.

extended – Specifies an extended IPv6 ACL.

acl-name – Name of the ACL. (Maximum length: 16 characters)

Command Mode

Privileged Exec

Example

```
Console#show ipv6 access-list standard
IPv6 standard access-list david:
  permit host 2009:DB9:2229::79
  permit 2009:DB9:2229:5::/64
Console#
```

Related Commands

[permit, deny \(Standard IPv6 ACL\) \(355\)](#)

[permit, deny \(Extended IPv6 ACL\) \(356\)](#)

[ipv6 access-group \(358\)](#)

ipv6 access-group This command binds a port to an IPv6 ACL. Use the **no** form to remove the port.

Syntax

ipv6 access-group *acl-name* **in** [**time-range** *time-range-name*]

no ipv6 access-group *acl-name* **in**

acl-name – Name of the ACL. (Maximum length: 16 characters)

in – Indicates that this list applies to ingress packets.

time-range-name - Name of the time range. (Range: 1-30 characters)

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ A port can only be bound to one ACL.
- ◆ If a port is already bound to an ACL and you bind it to a different ACL, the switch will replace the old binding with the new one.

Example

```
Console(config)#interface ethernet 1/2
Console(config-if)#ipv6 access-group standard david in
Console(config-if)#
```

Related Commands

[show ipv6 access-list \(357\)](#)

[Time Range \(169\)](#)

show ipv6 access-group This command shows the ports assigned to IPv6 ACLs.

Command Mode

Privileged Exec

Example

```
Console#show ipv6 access-group
Interface ethernet 1/2
  IPv6 standard access-list david in
Console#
```

Related Commands

[ipv6 access-group \(358\)](#)

MAC ACLs

The commands in this section configure ACLs based on hardware addresses, packet format, and Ethernet type. To configure MAC ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more ports.

Table 69: MAC ACL Commands

Command	Function	Mode
<code>access-list mac</code>	Creates a MAC ACL and enters configuration mode	GC
<code>permit, deny</code>	Filters packets matching a specified source and destination address, packet format, and Ethernet type	MAC-ACL
<code>mac access-group</code>	Binds a MAC ACL to a port	IC
<code>show mac access-group</code>	Shows port assignments for MAC ACLs	PE
<code>show mac access-list</code>	Displays the rules for configured MAC ACLs	PE

access-list mac This command adds a MAC access list and enters MAC ACL configuration mode. Use the **no** form to remove the specified ACL.

Syntax

[no] access-list mac *acl-name*

acl-name – Name of the ACL. (Maximum length: 16 characters, no spaces or other special characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list.
- ◆ To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- ◆ An ACL can contain up to 96 rules.

Example

```
Console(config)#access-list mac jerry
Console(config-mac-acl)#
```

Related Commands

[permit, deny \(360\)](#)

[mac access-group \(362\)](#)

[show mac access-list \(363\)](#)

permit, deny (MAC ACL) This command adds a rule to a MAC ACL. The rule filters packets matching a specified MAC source or destination address (i.e., physical layer address), or Ethernet protocol type. Use the **no** form to remove a rule.

Syntax

```
{permit | deny}  
  {any | host source | source address-bitmask}  
  {any | host destination | destination address-bitmask}  
  [vid vid vid-bitmask] [ethertype protocol [protocol-bitmask]]  
  [time-range time-range-name]
```

```
no {permit | deny}  
  {any | host source | source address-bitmask}  
  {any | host destination | destination address-bitmask}  
  [vid vid vid-bitmask] [ethertype protocol [protocol-bitmask]]
```



Note: The default is for Ethernet II packets.

```
{permit | deny} tagged-eth2  
  {any | host source | source address-bitmask}  
  {any | host destination | destination address-bitmask}  
  [vid vid vid-bitmask] [ethertype protocol [protocol-bitmask]]  
  [time-range time-range-name]
```

```
no {permit | deny} tagged-eth2  
  {any | host source | source address-bitmask}  
  {any | host destination | destination address-bitmask}  
  [vid vid vid-bitmask] [ethertype protocol [protocol-bitmask]]
```

```
{permit | deny} untagged-eth2  
  {any | host source | source address-bitmask}  
  {any | host destination | destination address-bitmask}  
  [ethertype protocol [protocol-bitmask]]  
  [time-range time-range-name]
```

```
no {permit | deny} untagged-eth2  
  {any | host source | source address-bitmask}  
  {any | host destination | destination address-bitmask}  
  [ethertype protocol [protocol-bitmask]]
```

```
{permit | deny} tagged-802.3  
  {any | host source | source address-bitmask}  
  {any | host destination | destination address-bitmask}  
  [vid vid vid-bitmask] [time-range time-range-name]
```


no {permit | deny} tagged-802.3

{**any** | **host** *source* | *source address-bitmask*}

{**any** | **host** *destination* | *destination address-bitmask*}

[**vid** *vid vid-bitmask*]

{permit | deny} untagged-802.3

{**any** | **host** *source* | *source address-bitmask*}

{**any** | **host** *destination* | *destination address-bitmask*}

[**time-range** *time-range-name*]

no {permit | deny} untagged-802.3

{**any** | **host** *source* | *source address-bitmask*}

{**any** | **host** *destination* | *destination address-bitmask*}

tagged-eth2 – Tagged Ethernet II packets.

untagged-eth2 – Untagged Ethernet II packets.

tagged-802.3 – Tagged Ethernet 802.3 packets.

untagged-802.3 – Untagged Ethernet 802.3 packets.

any – Any MAC source or destination address.

host – A specific MAC address.

source – Source MAC address.

destination – Destination MAC address range with bitmask.

*address-bitmask*⁵ – Bitmask for MAC address (in hexadecimal format).

vid – VLAN ID. (Range: 1-4094)

*vid-bitmask*⁵ – VLAN bitmask. (Range: 1-4095)

protocol – A specific Ethernet protocol number. (Range: 0-ffff hex.)

*protocol-bitmask*⁵ – Protocol bitmask. (Range: 0-ffff hex.)

time-range-name – Name of the time range. (Range: 1-30 characters)

Default Setting

None

Command Mode

MAC ACL

Command Usage

- ◆ New rules are added to the end of the list.
- ◆ The **ethertype** option can only be used to filter Ethernet II formatted packets.
- ◆ A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include the following:
 - 0800 - IP
 - 0806 - ARP

5. For all bitmasks, “1” means relevant and “0” means ignore.

- 8137 - IPX

Example

This rule permits packets from any source MAC address to the destination address 00-e0-29-94-34-de where the Ethernet type is 0800.

```
Console(config-mac-acl)#permit any host 00-e0-29-94-34-de ethertype 0800
Console(config-mac-acl)#
```

Related Commands

[access-list mac \(359\)](#)

[Time Range \(169\)](#)

mac access-group This command binds a MAC ACL to a port. Use the **no** form to remove the port.

Syntax

mac access-group *acl-name* **in** [**time-range** *time-range-name*]

acl-name – Name of the ACL. (Maximum length: 16 characters)

in – Indicates that this list applies to ingress packets.

time-range-name - Name of the time range. (Range: 1-30 characters)

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ Only one ACL can be bound to a port.
- ◆ If an ACL is already bound to a port and you bind a different ACL to it, the switch will replace the old binding with the new one.

Example

```
Console(config)#interface ethernet 1/2
Console(config-if)#mac access-group jerry in
Console(config-if)#
```

Related Commands

[show mac access-list \(363\)](#)

[Time Range \(169\)](#)

show mac access-group This command shows the ports assigned to MAC ACLs.

Command Mode
Privileged Exec

Example

```
Console#show mac access-group
Interface ethernet 1/5
  MAC access-list M5 in
Console#
```

Related Commands
[mac access-group \(362\)](#)

show mac access-list This command displays the rules for configured MAC ACLs.

Syntax

show mac access-list [*acl-name*]
acl-name – Name of the ACL. (Maximum length: 16 characters)

Command Mode
Privileged Exec

Example

```
Console#show mac access-list
MAC access-list jerry:
  permit any 00-e0-29-94-34-de ethertype 0800
Console#
```

Related Commands
[permit, deny \(360\)](#)
[mac access-group \(362\)](#)

ARP ACLs

The commands in this section configure ACLs based on the IP or MAC address contained in ARP request and reply messages. To configure ARP ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more VLANs using the `ip arp inspection vlan` command.

Table 70: ARP ACL Commands

Command	Function	Mode
<code>access-list arp</code>	Creates a ARP ACL and enters configuration mode	GC
<code>permit, deny</code>	Filters packets matching a specified source or destination address in ARP messages	ARP-ACL
<code>show arp access-list</code>	Displays the rules for configured ARP ACLs	PE

access-list arp This command adds an ARP access list and enters ARP ACL configuration mode. Use the **no** form to remove the specified ACL.

Syntax

[no] access-list arp *acl-name*

acl-name – Name of the ACL. (Maximum length: 16 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list. To create an ACL, you must add at least one rule to the list.
- ◆ To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- ◆ An ACL can contain up to 96 rules.

Example

```
Console(config)#access-list arp factory
Console(config-arp-acl)#
```

Related Commands

[permit, deny \(365\)](#)

[show arp access-list \(366\)](#)

permit, deny (ARP ACL) This command adds a rule to an ARP ACL. The rule filters packets matching a specified source or destination address in ARP messages. Use the **no** form to remove a rule.

Syntax

```
[no] {permit | deny}
    ip {any | host source-ip | source-ip ip-address-bitmask}
    mac {any | host source-mac | source-mac mac-address-bitmask} [log]
```

This form indicates either request or response packets.

```
[no] {permit | deny} request
    ip {any | host source-ip | source-ip ip-address-bitmask}
    mac {any | host source-mac | source-mac mac-address-bitmask} [log]
```

```
[no] {permit | deny} response
    ip {any | host source-ip | source-ip ip-address-bitmask}
    {any | host destination-ip | destination-ip ip-address-bitmask}
    mac {any | host source-mac | source-mac mac-address-bitmask}
    [any | host destination-mac | destination-mac mac-address-bitmask] [log]
```

source-ip – Source IP address.

destination-ip – Destination IP address with bitmask.

*ip-address-bitmask*⁶ – IPv4 number representing the address bits to match.

source-mac – Source MAC address.

destination-mac – Destination MAC address range with bitmask.

*mac-address-bitmask*⁶ – Bitmask for MAC address (in hexadecimal format).

log - Logs a packet when it matches the access control entry.

Default Setting

None

Command Mode

ARP ACL

Command Usage

New rules are added to the end of the list.

Example

This rule permits packets from any source IP and MAC address to the destination subnet address 192.168.0.0.

```
Console(config-arp-acl)#$permit response ip any 192.168.0.0 255.255.0.0 mac
any any
Console(config-mac-acl)#
```

6. For all bitmasks, binary “1” means relevant and “0” means ignore.

Related Commands

[access-list arp \(364\)](#)

show arp access-list This command displays the rules for configured ARP ACLs.

Syntax

show arp access-list [*acl-name*]

acl-name – Name of the ACL. (Maximum length: 16 characters)

Command Mode

Privileged Exec

Example

```
Console#show arp access-list
ARP access-list factory:
  permit response ip any 192.168.0.0 255.255.0.0 mac any any
Console#
```

Related Commands

[permit, deny \(365\)](#)

ACL Information

This section describes commands used to display ACL information.

Table 71: ACL Information Commands

Command	Function	Mode
show access-group	Shows the ACLs assigned to each port	PE
show access-list	Show all ACLs and associated rules	PE

show access-group This command shows the port assignments of ACLs.

Command Mode

Privileged Executive

Example

```
Console#show access-group
Interface ethernet 1/2
  IP access-list david
  MAC access-list jerry
Console#
```

show access-list This command shows all ACLs and associated rules.

Syntax

show access-list

```
[[arp [acl-name]] |  
ip extended [acl-name] | standard [acl-name]] |  
ipv6 extended [acl-name] | standard [acl-name]] |  
mac [acl-name]] | [tcam-utilization]
```

arp – Shows ingress or egress rules for ARP ACLs.

ip extended – Shows ingress rules for Extended IPv4 ACLs.

ip standard – Shows ingress rules for Standard IPv4 ACLs.

ipv6 extended – Shows ingress rules for Extended IPv6 ACLs.

ipv6 standard – Shows ingress rules for Standard IPv6 ACLs.

mac – Shows ingress rules for MAC ACLs.

tcam-utilization – Shows the percentage of user configured ACL rules as a percentage of total ACL rules

acl-name – Name of the ACL. (Maximum length: 16 characters)

Command Mode

Privileged Exec

Example

```
Console#show access-list  
IP standard access-list david:  
  permit host 10.1.1.21  
  permit 168.92.0.0 255.255.15.0  
IP extended access-list bob:  
  permit 10.7.1.1 255.255.255.0 any  
  permit 192.168.1.0 255.255.255.0 any destination-port 80 80  
  permit 192.168.1.0 255.255.255.0 any protocol tcp control-code 2 2  
MAC access-list jerry:  
  permit any host 00-30-29-94-34-de ethertype 800 800  
IP extended access-list A6:  
  deny tcp any any control-flag 2 2  
  permit any any  
Console#
```


Interface Commands

These commands are used to display or set communication parameters for an Ethernet port, aggregated link, or VLAN; or perform cable diagnostics on the specified interface.

Table 72: Interface Commands

Command	Function	Mode
<i>Interface Configuration</i>		
<code>interface</code>	Configures an interface type and enters interface configuration mode	GC
<code>alias</code>	Configures an alias name for the interface	IC
<code>capabilities</code>	Advertises the capabilities of a given interface for use in autonegotiation	IC
<code>description</code>	Adds a description to an interface configuration	IC
<code>flowcontrol</code>	Enables flow control on a given interface	IC
<code>history</code>	Configures a periodic sampling of statistics, specifying the sampling interval and number of samples	IC
<code>negotiation</code>	Enables autonegotiation of a given interface	IC
<code>shutdown</code>	Disables an interface	IC
<code>switchport block</code>	Prevents flooding of broadcast, unknown multicast, or unknown unicast packets	IC
<code>switchport mtu</code>	Sets the maximum transfer unit for an interface	IC
<code>transceiver-threshold-auto</code>	Uses default threshold settings obtained from the transceiver to determine when an alarm or trap message should be sent	IC
<code>transceiver-monitor</code>	Sends a trap when any of the transceiver's operational values fall outside specified thresholds	IC
<code>transceiver-threshold current</code>	Sets thresholds for transceiver current which can be used to trigger an alarm or warning message	IC
<code>transceiver-threshold rx-power</code>	Sets thresholds for the transceiver power level of the received signal which can be used to trigger an alarm or warning message	IC
<code>transceiver-threshold temperature</code>	Sets thresholds for the transceiver temperature which can be used to trigger an alarm or warning message	IC
<code>transceiver-threshold tx-power</code>	Sets thresholds for the transceiver power level of the transmitted signal which can be used to trigger an alarm or warning message	IC
<code>transceiver-threshold voltage</code>	Sets thresholds for the transceiver voltage which can be used to trigger an alarm or warning message	IC
<code>clear counters</code>	Clears statistics on an interface	PE

Table 72: Interface Commands (Continued)

Command	Function	Mode
show interfaces brief	Displays a summary of key information, including operational status, native VLAN ID, default priority, speed/duplex mode, and port type	PE
show interfaces counters	Displays statistics for the specified interfaces	NE, PE
show interfaces history	Displays statistical history for the specified interfaces	PE
show interfaces status	Displays status for the specified interface	NE, PE
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE
show interfaces transceiver	Displays the temperature, voltage, bias current, transmit power, and receive power	PE
show interfaces transceiver-threshold	Displays the alarm/warning thresholds for temperature, voltage, bias current, transmit power, and receive power	PE
<i>Cable Diagnostics</i>		
test loop internal	Performs an internal loop back test on the specified port	PE
show loop internal	Shows the results of a loop back test	PE

Interface Configuration

interface This command configures an interface type and enters interface configuration mode. Use the **no** form with a trunk to remove an inactive interface.

Syntax

[no] interface *interface-list*

interface-list – One or more ports. Use a hyphen to indicate a consecutive list of ports or a comma between non-consecutive ports.

craft - Management port on the front panel.

ethernet *unit/port-list*

unit - Unit identifier. (Range: 1)

port-list - Physical port number or list of port numbers. Separate nonconsecutive port numbers with a comma and no spaces; or use a hyphen to designate a range of port numbers. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

tunnel *tunnel-number*. (Range: 1-16)

See the [interface tunnel](#) command.

vlan *vlan-id* (Range: 1-4094)

Default Setting

None

Command Mode

Global Configuration

Command Usage

The craft interface is provided as an out-of-band management connection which is isolated from all other ports on the switch. This interface must first be configured with an IPv4 or IPv6 address before a connection can be made through Telnet, SSH, or HTTP.

Example

To specify port 4, enter the following command:

```
Console(config)#interface ethernet 1/4
Console(config-if)#
```

alias This command configures an alias name for the interface. Use the **no** form to remove the alias name.

Syntax

alias *string*

no alias

string - A mnemonic name to help you remember what is attached to this interface. (Range: 1-64 characters)

Default Setting

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

The alias is displayed in the running-configuration file. An example of the value which a network manager might store in this object for a WAN interface is the (Telco's) circuit number/identifier of the interface.

Example

The following example adds an alias to port 4.

```
Console(config)#interface ethernet 1/4
Console(config-if)#alias finance
Console(config-if)#
```

capabilities This command advertises the port capabilities of a given interface during auto-negotiation. Use the **no** form with parameters to remove an advertised capability, or the **no** form without parameters to restore the default values.

Syntax

[no] capabilities {flowcontrol | symmetric}

flowcontrol (Gigabit SFP only) - Supports flow control.

symmetric (Gigabit SFP only) - When specified, the port transmits and receives symmetric pause frames.

Default Setting

100Base-FX (SFP): 100full

1000BASE-SX/LX (SFP): 1000full

10GBASE-CR/SR/LR/LRM (SFP+): 10Gfull

40GBASE-T-CR4 (QSFP+): 40Gfull

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ 10GBASE-SFP+ connections are fixed at 10G - full duplex, and 40GBASE-QSFP+ connections at 40G - full duplex. Auto-negotiation must be disabled before you can configure or force an RJ-45 interface to use the Flow Control option.
- ◆ When auto-negotiation is enabled with the [negotiation](#) command⁷, the switch will negotiate the best settings for a link based on the **capabilities** command. When auto-negotiation is disabled, you must manually specify the link attributes with the [flowcontrol](#) command.

Example

The following example configures Ethernet port 5 capabilities to include 100half and 100full.

```
Console(config)#interface ethernet 1/5
Console(config-if)#capabilities flowcontrol
Console(config-if)#
```

Related Commands

[negotiation \(375\)](#)

[flowcontrol \(373\)](#)

7. Support for auto-negotiation depends on transceiver type, such as 1G SFP.

description This command adds a description to an interface. Use the **no** form to remove the description.

Syntax

description *string*

no description

string - Comment or a description to help you remember what is attached to this interface. (Range: 1-64 characters)

Default Setting

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

The description is displayed by the [show interfaces status](#) command and in the running-configuration file. An example of the value which a network manager might store in this object is the name of the manufacturer, and the product name.

Example

The following example adds a description to port 4.

```
Console(config)#interface ethernet 1/4
Console(config-if)#description RD-SW#3
Console(config-if)#
```

flowcontrol This command enables flow control. Use the **no** form to disable flow control.

Syntax

[no] flowcontrol

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ 10GBASE-SFP+ and 40GBASE-QSFP transceivers do not support auto-negotiation. Forced mode should always be used to establish a connection over any 10GBASE-SFP+ or 10GBASE-SFP+ port or trunk.
- ◆ Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled,

back pressure is used for half-duplex operation and IEEE 802.3-2002 (formally IEEE 802.3x) for full-duplex operation.

- ◆ To force flow control on or off (with the **flowcontrol** or **no flowcontrol** command), use the **no negotiation** command to disable auto-negotiation on the selected interface.
- ◆ When using the **negotiation** command to enable auto-negotiation, the optimal settings will be determined by the **capabilities** command. To enable flow control under auto-negotiation, “flowcontrol” must be included in the capabilities list for any port

Example

The following example enables flow control on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#flowcontrol
Console(config-if)#no negotiation
Console(config-if)#
```

Related Commands

negotiation (375)

capabilities (flowcontrol, symmetric) (372)

history This command configures a periodic sampling of statistics, specifying the sampling interval and number of samples. Use the **no** form to remove a named entry from the sampling table.

Syntax

history *name interval buckets*

no history *name*

name - A symbolic name for this entry in the sampling table. (Range: 1-32 characters)

interval - The interval for sampling statistics. (Range: 1-86400 seconds)

buckets - The number of samples to take. (Range: 1-96)

Default Setting

15min - 15 minute interval, 96 buckets

1day - 1 day interval, 7 buckets

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

This example sets a interval of 15 minutes for sampling standard statistical values on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#history 15min 15 10
Console(config-if)#
```

negotiation This command enables auto-negotiation for a given interface. Use the **no** form to disable auto-negotiation.

Syntax

[no] negotiation

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ The 10GBASE-SFP+ and 40GBASE-QSFP transceivers do not support auto-negotiation. Forced mode should always be used to establish a connection over any 10GBASE-SFP or 40GBASE-QSFP port or trunk.
- ◆ When auto-negotiation is enabled⁸ the switch will negotiate the best settings for a link based on the [capabilities](#) command. When autonegotiation is disabled, you must manually specify the link attributes with the [flowcontrol](#) command.
- ◆ A connection can only be enabled on a port in which a recognized transceiver is inserted. Refer to the *Installation Guide* for a list of compliant transceivers.

Example

The following example configures port 10 to use auto-negotiation.

```
Console(config)#interface ethernet 1/10
Console(config-if)#negotiation
Console(config-if)#
```

Related Commands

[capabilities \(372\)](#)

[flowcontrol \(373\)](#)

8. Support for auto-negotiation depends on transceiver type, such as 1G SFP.

shutdown This command disables an interface. To restart a disabled interface, use the **no** form.

Syntax

[no] shutdown

Default Setting

All interfaces are enabled.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This command allows you to disable a port due to abnormal behavior (e.g., excessive collisions), and then re-enable it after the problem has been resolved. You may also want to disable a port for security reasons.

Example

The following example disables port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#shutdown
Console(config-if)#
```

switchport block This command prevents the flooding of broadcast, unknown multicast, or unknown unicast packets onto an interface. Use the **no** form to restore the default setting.

Syntax

[no] switchport block {broadcast | multicast | unicast}

broadcast - Specifies broadcast packets.

multicast - Specifies unknown multicast packets.

unicast - Specifies unknown unicast packets.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Default Setting

Disabled

Command Usage

By default, broadcast, unknown multicast, and unknown unicast traffic is flooded to all ports. This occurs if a MAC address has been timed out or not yet learned by the switch. If this kind of traffic is flooded to an isolated port on a private VLAN, there could be security issues.

Example

The following example blocks unknown multicast traffic on port 5:

```
Console(config)#interface ethernet 1/5
Console(config-if)#switchport switchport block multicast
Console(config-if)#
```

switchport mtu This command configures the maximum transfer unit (MTU) allowed for layer 2 packets crossing a Gigabit, 10 Gigabit or 40 Gigabit Ethernet port or trunk. Use the **no** form to restore the default setting.

Syntax

switchport mtu *size*

no switchport mtu

size - Specifies the maximum transfer unit (or frame size) for a Gigabit, 10 Gigabit or 40 Gigabit Ethernet port or trunk. (Range: 1500-12288 bytes)

Default Setting

1518 bytes

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ Use the [jumbo frame](#) command to enable or disable jumbo frames for all Gigabit, 10 Gigabit and 40 Gigabit Ethernet ports. To set the MTU for a specific interface, enable jumbo frames and use this command to specify the required size of the MTU.
- ◆ The comparison of packet size against the configured port MTU considers only the incoming packet size, and is not affected by the fact that an ingress port is a tagged port or a QinQ ingress port. In other words, any additional size (for example, a tagged field of 4 bytes added by the chip) will not be considered when comparing the egress packet's size against the configured MTU.
- ◆ When pinging the switch from an external device, information added for the Ethernet header can increase the packet size by at least 42 bytes for an untagged packet, and 46 bytes for a tagged packet. If the adjusted frame size exceeds the configured port MTU, the switch will not respond to the ping message.
- ◆ For other traffic types, calculation of overall frame size is basically the same, including the additional header fields SA(6) + DA(6) + Type(2) + VLAN-Tag(4) (for tagged packets, for untagged packets, the 4-byte field will not be added by switch), and the payload. This should all be less than the configured port MTU, including the CRC at the end of the frame.
- ◆ For QinQ, the overall frame size is still calculated as described above, and does not add the length of the second tag to the frame.
- ◆ The port MTU size can be displayed with the show [show interfaces status](#) command.

Example

The following first enables jumbo frames for layer 2 packets, and then sets the MTU for port 1:

```
Console(config)#jumbo frame
Console(config)#interface ethernet 1/1
Console(config-if)#switchport mtu 9216
Console(config-if)#
```

Related Commands

[jumbo frame \(122\)](#)

[show interfaces status \(393\)](#)

transceiver-threshold-auto This command uses default threshold settings obtained from the transceiver to determine when an alarm or warning message should be sent. Use the **no** form to disable this feature.

Syntax

transceiver-threshold-auto

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet)

Example

```
Console(config)interface ethernet 1/1
Console(config-if)#transceiver-threshold-auto
Console#
```

transceiver-monitor This command sends a trap when any of the transceiver's operational values fall outside of specified thresholds. Use the **no** form to disable trap messages.

Syntax

transceiver-monitor

Default Setting

[Disabled](#)

Command Mode

Interface Configuration (Ethernet)

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#transceiver-monitor
Console#
```

transceiver-threshold current This command sets thresholds for transceiver current which can be used to trigger an alarm or warning message.

Syntax

transceiver-threshold current {high-alarm | high-warning | low-alarm | low-warning} threshold-value

high-alarm – Sets the high current threshold for an alarm message.

high-warning – Sets the high current threshold for a warning message.

low-alarm – Sets the low current threshold for an alarm message.

low-warning – Sets the low current threshold for a warning message.

threshold-value – The threshold of the transceiver current.
(Range: 100-25500 in units of 0.01 mA)

Default Setting

High Alarm: 100 mA
High Warning: 90 mA
Low Warning: 7 mA
Low Alarm: 6 mA

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ If trap messages are enabled with the [transceiver-monitor](#) command, and a high-threshold alarm or warning message is sent if the current value is greater than or equal to the threshold, and the last sample value was less than the threshold. After a rising event has been generated, another such event will not be generated until the sampled value has fallen below the high threshold and reaches the low threshold.
- ◆ If trap messages are enabled with the [transceiver-monitor](#) command, and a low-threshold alarm or warning message is sent if the current value is less than or equal to the threshold, and the last sample value was greater than the threshold. After a falling event has been generated, another such event will not be generated until the sampled value has risen above the low threshold and reaches the high threshold.
- ◆ Threshold events are triggered as described above to avoid a hysteresis effect which would continuously trigger event messages if the power level were to fluctuate just above and below either the high threshold or the low threshold.

- ◆ Trap messages enabled by the [transceiver-monitor](#) command are sent to any management station configured by the [snmp-server host](#) command.

Example

The following example sets alarm thresholds for the transceiver current at port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#transceiver-threshold current low-alarm 100
Console(config-if)#transceiver-threshold rx-power high-alarm 700
Console#
```

transceiver-threshold rx-power This command sets thresholds for the transceiver power level of the received signal which can be used to trigger an alarm or warning message.

Syntax

transceiver-threshold rx-power {high-alarm | high-warning | low-alarm | low-warning} threshold-value

high-alarm – Sets the high power threshold for an alarm message.

high-warning – Sets the high power threshold for a warning message.

low-alarm – Sets the low power threshold for an alarm message.

low-warning – Sets the low power threshold for a warning message.

threshold-value – The power threshold of the received signal.
(Range: -9999 - 9999 in units of 0.01 dBm)

Default Setting

High Alarm: -3.00 dBm
High Warning: -3.50 dBm
Low Warning: -21.00 dBm
Low Alarm: -21.50 dBm

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ The threshold value is the power ratio in decibels (dB) of the measured power referenced to one milliwatt (mW).
- ◆ Refer to the Command Usage section under the [transceiver-threshold current](#) command for more information on configuring transceiver thresholds.
- ◆ Trap messages enabled by the [transceiver-monitor](#) command are sent to any management station configured by the [snmp-server host](#) command.

Example

The following example sets alarm thresholds for the signal power received at port 1.

```
Console(config)interface ethernet 1/1
Console(config-if)#transceiver-threshold rx-power low-alarm -21
Console(config-if)#transceiver-threshold rx-power high-alarm -3
Console#
```

transceiver-threshold temperature This command sets thresholds for the transceiver temperature which can be used to trigger an alarm or warning message.

Syntax

transceiver-threshold temperature {high-alarm | high-warning | low-alarm | low-warning} threshold-value

high-alarm – Sets the high temperature threshold for an alarm message.

high-warning – Sets the high temperature threshold for a warning message.

low-alarm – Sets the low temperature threshold for an alarm message.

low-warning – Sets the low temperature threshold for a warning message.

threshold-value – The threshold of the transceiver temperature.
(Range: -20000 - 20000 in units of 0.01 Celsius)

Default Setting

High Alarm: 75.00 °C
High Warning: 70.00 °C
Low Alarm: -123.00 °C
Low Warning: 0.00 °C

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ Refer to the Command Usage section under the [transceiver-threshold current](#) command for more information on configuring transceiver thresholds.
- ◆ Trap messages enabled by the [transceiver-monitor](#) command are sent to any management station configured by the [snmp-server host](#) command.

Example

The following example sets alarm thresholds for the transceiver temperature at port 1.

```
Console(config)interface ethernet 1/1
Console(config-if)#transceiver-threshold temperature low-alarm 97
```

```
Console(config-if)#transceiver-threshold temperature high-alarm -83
Console#
```

transceiver-threshold tx-power This command sets thresholds for the transceiver power level of the transmitted signal which can be used to trigger an alarm or warning message.

Syntax

transceiver-threshold tx-power {high-alarm | high-warning | low-alarm | low-warning} threshold-value

high-alarm – Sets the high power threshold for an alarm message.

high-warning – Sets the high power threshold for a warning message.

low-alarm – Sets the low power threshold for an alarm message.

low-warning – Sets the low power threshold for a warning message.

threshold-value – The power threshold of the transmitted signal.
(Range: -9999 - 9999 in units of 0.01 dBm)

Default Setting

High Alarm: -9.00 dBm
High Warning: -9.50 dBm
Low Warning: -21.00 dBm
Low Alarm: -21.50 dBm

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ The threshold value is the power ratio in decibels (dB) of the measured power referenced to one milliwatt (mW).
- ◆ Refer to the Command Usage section under the [transceiver-threshold current](#) command for more information on configuring transceiver thresholds.
- ◆ Trap messages enabled by the [transceiver-monitor](#) command are sent to any management station configured by the [snmp-server host](#) command.

Example

The following example sets alarm thresholds for the signal power transmitted at port 1.

```
Console(config)interface ethernet 1/1
Console(config-if)#transceiver-threshold tx-power low-alarm 8
Console(config-if)#transceiver-threshold tx-power high-alarm -3
Console#
```

transceiver-threshold voltage This command sets thresholds for the transceiver voltage which can be used to trigger an alarm or warning message.

Syntax

transceiver-threshold voltage {**high-alarm** | **high-warning** | **low-alarm** | **low-warning**} *threshold-value*

high-alarm – Sets the high voltage threshold for an alarm message.

high-warning – Sets the high voltage threshold for a warning message.

low-alarm – Sets the low voltage threshold for an alarm message.

low-warning – Sets the low voltage threshold for a warning message.

threshold-value – The threshold of the transceiver voltage.

(Range: 100-25500 in units of 0.01 Volt)

Default Setting

High Alarm: 3.50 Volts

High Warning: 3.45 Volts

Low Warning: 3.15 Volts

Low Alarm: 3.10 Volts

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ Refer to the Command Usage section under the [transceiver-threshold current](#) command for more information on configuring transceiver thresholds.
- ◆ Trap messages enabled by the [transceiver-monitor](#) command are sent to any management station configured by the [snmp-server host](#) command.

Example

The following example sets alarm thresholds for the transceiver voltage at port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#transceiver-threshold voltage low-alarm 4
Console(config-if)#transceiver-threshold voltage high-alarm 2
Console#
```


clear counters This command clears statistics on an interface.

Syntax

clear counters *interface*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Statistics are only initialized for a power reset. This command sets the base value for displayed statistics to zero for the current management session. However, if you log out and back into the management interface, the statistics displayed will show the absolute value accumulated since the last power reset.

Example

The following example clears statistics on port 5.

```
Console#clear counters ethernet 1/5
Console#
```

show interfaces brief This command displays a summary of key information, including operational status, native VLAN ID, default priority, speed/duplex mode, and port type for all ports.

Command Mode

Privileged Exec

Example

```
Console#show interfaces brief
Interface Name      Status      PVID Pri Speed/Duplex  Type      Trunk
-----
Eth 1/ 1           Up          1    0 Auto-1000full 1000BASE SFP None
Eth 1/ 2           Up          1    0 1000full      1000BASE SFP None
Eth 1/ 3           Down        1    0 10Gfull       10GBASE SFP+ None
:
```

show interfaces counters This command displays interface statistics.

Syntax

```
show interfaces counters [interface]  
interface  
ethernet unit/port  
unit - Unit identifier. (Range: 1)  
port - Port number. (Range: 1-52)  
port-channel channel-id (Range: 1-8)
```

Default Setting

Shows the counters for all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed.

Example

```
Console#show interfaces counters ethernet 1/1  
Ethernet 1/ 1  
===== IF table Stats =====  
2166458 Octets Input  
14734059 Octets Output  
14707 Unicast Input  
19806 Unicast Output  
0 Discard Input  
0 Discard Output  
0 Error Input  
0 Error Output  
0 Unknown Protocols Input  
0 QLen Output  
===== Extended Iftable Stats =====  
23 Multi-cast Input  
5525 Multi-cast Output  
170 Broadcast Input  
11 Broadcast Output  
===== Ether-like Stats =====  
0 Alignment Errors  
0 FCS Errors  
0 Single Collision Frames  
0 Multiple Collision Frames  
0 SQE Test Errors  
0 Deferred Transmissions  
0 Late Collisions  
0 Excessive Collisions  
0 Internal Mac Transmit Errors  
0 Internal Mac Receive Errors  
0 Frames Too Long  
0 Carrier Sense Errors  
0 Symbol Errors
```

```

0 Pause Frames Input
0 Pause Frames Output
===== RMON Stats =====
0 Drop Events
16900558 Octets
40243 Packets
170 Broadcast PKTS
23 Multi-cast PKTS
0 Undersize PKTS
0 Oversize PKTS
0 Fragments
0 Jabbers
0 CRC Align Errors
0 Collisions
21065 Packet Size <= 64 Octets
3805 Packet Size 65 to 127 Octets
2448 Packet Size 128 to 255 Octets
797 Packet Size 256 to 511 Octets
2941 Packet Size 512 to 1023 Octets
9187 Packet Size 1024 to 1518 Octets
===== Port Utilization =====
111 Octets Input per seconds
0 Packets Input per seconds
0.00 % Input Utilization
606 Octets Output per seconds
1 Packets Output per second
0.00 % Output Utilization

Console#

```

Table 73: show interfaces counters - display description

Parameter	Description
<i>IF Table Stats</i>	
Octets Input	The total number of octets received on the interface, including framing characters.
Octets Output	The total number of octets transmitted out of the interface, including framing characters.
Unicast Input	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Unicast Output	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Discard Input	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Discard Output	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Error Input	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Error Output	The number of outbound packets that could not be transmitted because of errors.
Unknown Protocols Input	The number of packets received which were discarded because of an unknown or unsupported protocol.

Table 73: show interfaces counters - display description (Continued)

Parameter	Description
QLen Output	The length of the output packet queue (in packets).
<i>Extended IF Table Stats</i>	
Multicast Input	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer.
Multicast Output	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
Broadcast Input	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer.
Broadcast Output	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.
<i>Etherlike Statistics</i>	
Alignment Errors	The number of alignment errors (missynchronized data packets).
FCS Errors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.
Single Collision Frames	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Multiple Collision Frames	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
SQE Test Errors	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface.
Deferred Transmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
Excessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increment when the interface is operating in full-duplex mode.
Internal MAC Transmit Errors	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error.
Internal MAC Receive Errors	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error.
Frames Too Long	A count of frames received on a particular interface that exceed the maximum permitted frame size.
Carrier Sense Errors	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.

Table 73: show interfaces counters - display description (Continued)

Parameter	Description
Symbol Errors	<p>For an interface operating at 100 Mb/s, the number of times there was an invalid data symbol when a valid carrier was present.</p> <p>For an interface operating in half-duplex mode at 1000 Mb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than slotTime, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Data reception error' or 'carrier extend error' on the GMII.</p> <p>For an interface operating in full-duplex mode at 1000 Mb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than minFrameSize, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Data reception error' on the GMII</p>
<i>RMON Statistics</i>	
Octets	Total number of octets of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Packets	The total number of packets (bad, broadcast and multicast) received.
Broadcast Packets	The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Multicast Packets	The total number of good packets received that were directed to this multicast address.
Undersize Packets	The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize Packets	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.
<i>CRC Align Errors</i>	
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
64 Octets	The total number of packets (including bad packets) received and transmitted that were less than 64 octets in length (excluding framing bits but including FCS octets).
65-127 Octets	The total number of packets (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).
128-255 Octets	
256-511 Octets	
512-1023 Octets	
1024-1518 Octets	
1519-1536 Octets	
<i>Utilization Statistics</i>	
Octets input per second	Number of octets entering this interface in kbits per second.
Packets input per second	Number of packets entering this interface in packets per second.

Table 73: show interfaces counters - display description (Continued)

Parameter	Description
Input utilization	The input utilization rate for this interface.
Octets output per second	Number of octets leaving this interface in kbits per second.
Packets output per second	Number of packets leaving this interface in packets per second.
Output utilization	The output utilization rate for this interface.

show interfaces history

This command displays statistical history for the specified interfaces.

show interfaces history [*interface* [*name* [**current** | **previous** *index count*] [**input** | **output**]]]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

name - Name of sample as defined in the [history](#) command.
(Range: 1-32 characters)

current - Statistics recorded in current interval.

previous - Statistics recorded in previous intervals.

index - An index into the buckets containing previous samples.
(Range: 1-96)

count - The number of historical samples to display. (Range: 1-96)

input - Ingress traffic.

output - Egress traffic.

Default Setting

Shows historical statistics for all interfaces, intervals, ingress traffic, and egress traffic.

Command Mode

Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed.

Example

This example shows the statistics recorded for all named entries in the sampling table.

```

Console#show interfaces history ethernet 1/1
Interface      : Eth 1/ 1
Name           : 15min
Interval       : 900 second(s)
Buckets Requested : 96
Buckets Granted  : 7
Status         : Active

Current Entries

Start Time    %      Octets Input  Unicast      Multicast     Broadcast
-----
00d 01:45:01  0.00      105421      688          30            8

Discards      Errors      Unknown Proto
-----
0              0              0

%      Octets Output  Unicast      Multicast     Broadcast
-----
0.00      859987          947          373            1

Discards      Errors
-----
0              0

Interface      : Eth 1/ 1
Name           : 1day
Interval       : 86400 second(s)
Buckets Requested : 7
Buckets Granted  : 0
Status         : Active

Current Entries

Start Time    %      Octets Input  Unicast      Multicast     Broadcast
-----
00d 00:00:00  0.00      969845      6548         237            82

Discards      Errors      Unknown Proto
-----
7              0              0

%      Octets Output  Unicast      Multicast     Broadcast
-----
0.00      8455699          9101         3146            3

Discards      Errors
-----
0              0

Console#

```

This example shows the statistics recorded for a named entry in the sampling table.

```

Console#show interfaces history ethernet 1/1 1min
Interface       : Eth 1/ 1
Name            : 1min
Interval        : 60 second(s)
Buckets Requested : 10
Buckets Granted  : 1
Status          : Active

Current Entries

Start Time  %      Octets Input  Unicast      Multicast      Broadcast
-----
00d 02:00:31  0.00          5856          39            1              0

Discards      Errors      Unknown Proto
-----
0              0              0

%      Octets Output  Unicast      Multicast      Broadcast
-----
0.00          48334          54            19              0

Discards      Errors
-----
0              0

Previous Entries

Start Time  Octets Input  Unicast      Multicast      Broadcast
-----
00d 00:05:37  1400912      9381          1895           50
00d 00:06:37  1566090      10660         2195           50
00d 00:07:37  1754781      11786         2674           59

Start Time  Octets Input  Discards      Errors      Unknown Proto
-----
00d 00:05:37  1400912      0              0            0
00d 00:06:37  1566090      0              0            0
00d 00:07:37  1754781      0              0            0

Start Time  Octets Output  Unicast      Multicast      Broadcast
-----
00d 00:05:37  6827866      10563         2042           30
00d 00:06:37  7572668      12040         2362           30
00d 00:07:37  8548505      13380         2879           30

Start Time  Octets Output  Discards      Errors
-----
00d 00:05:37  6827866      0              0
00d 00:06:37  7572668      0              0
00d 00:07:37  8548505      0              0

Console#

```


show interfaces status This command displays the status for an interface.

Syntax

show interfaces status [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

vlan *vlan-id* (Range: 1-4094)

Default Setting

Shows the status for all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed.

Example

```
Console#show interfaces status ethernet 1/1
Information of Eth 1/1
Basic Information:
  Port Type           : 1000Base SFP
  MAC Address         : 00-00-0C-00-00-FE
Configuration:
  Name                 :
  Port Admin           : Up
  Speed-duplex         : Auto
  Capabilities         : 1000full
  Broadcast Storm      : Enabled
  Broadcast Storm Limit : 500 packets/second
  Multicast Storm       : Disabled
  Multicast Storm Limit : 262143 packets/second
  Unknown Unicast Storm : Disabled
  Unknown Unicast Storm Limit : 262143 packets/second
  Flow Control         : Disabled
  VLAN Trunking        : Disabled
  LACP                 : Disabled
  MAC-Learning         : Yes
  Media Type           : None
  MTU                  : 1518
Current Status:
  Link Status          : Up
  Port Operation Status : Up
  Operation Speed-duplex : 1000full
  Up Time              : 0w 0d 1h 41m 8s (6068 seconds)
  Flow Control Type     : None
  Max Frame Size        : 1518 bytes (1522 bytes for tagged frames)
  MAC Learning Status   : Enabled
Console#
```

show interfaces switchport This command displays the administrative and operational status of the specified interfaces.

Syntax

show interfaces switchport [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Default Setting

Shows all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed.

Example

This example shows the configuration setting for port 1.

```
Console#show interfaces switchport ethernet 1/1
Information of Eth 1/1
Broadcast Threshold           : Enabled, 500 packets/second
Multicast Threshold           : Disabled
Unknown Unicast Threshold     : Disabled
LACP Status                   : Disabled
Ingress Rate Limit            : Disabled, 1000000 Kbits per second
Egress Rate Limit             : Disabled, 1000000 Kbits per second
VLAN Membership Mode          : Hybrid
Ingress Rule                  : Disabled
Acceptable Frame Type         : All frames
Native VLAN                   : 1
Priority for Untagged Traffic  : 0
GVRP Status                   : Disabled
Allowed VLAN                   : 1(u)
Forbidden VLAN                 : 
Private-VLAN Mode             : None
Private-VLAN host-association : None
Private-VLAN Mapping          : None
802.1Q Tunnel Status          : Disabled
802.1Q Tunnel Mode            : Normal
802.1Q Tunnel TPID            : 8100 (Hex)
Layer 2 Protocol Tunnel       : None
Broadcast Block                : Disabled
Unknown Multicast Block       : Disabled
Unknown Unicast Block         : Disabled
Console#
```

Table 74: show interfaces switchport - display description

Field	Description
Broadcast Threshold	Shows if broadcast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 427).
Multicast Threshold	Shows if multicast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 427).
Unknown Unicast Threshold	Shows if unknown unicast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 427).
LACP Status	Shows if Link Aggregation Control Protocol has been enabled or disabled (page 404).
Ingress/Egress Rate Limit	Shows if rate limiting is enabled, and the current rate limit (page 426).
VLAN Membership Mode	Indicates membership mode as Trunk or Hybrid (page 489).
Ingress Rule	Shows if ingress filtering is enabled or disabled (page 489).
Acceptable Frame Type	Shows if acceptable VLAN frames include all types or tagged frames only (page 487).
Native VLAN	Indicates the default Port VLAN ID (page 490).
Priority for Untagged Traffic	Indicates the default priority for untagged frames (page 530).
GVRP Status	Shows if GARP VLAN Registration Protocol is enabled or disabled (page 480).
Allowed VLAN	Shows the VLANs this interface has joined, where “(u)” indicates untagged and “(t)” indicates tagged (page 488).
Forbidden VLAN	Shows the VLANs this interface can not dynamically join via GVRP (page 480).
Private-VLAN Mode	Shows the private VLAN mode as host, promiscuous, or none (509).
Private VLAN host-association	Shows the secondary (or community) VLAN with which this port is associated (509).
Private VLAN mapping	Shows the primary VLAN mapping for a promiscuous port (511).
802.1Q-tunnel Status	Shows if 802.1Q tunnel is enabled on this interface (page 494).
802.1Q-tunnel Mode	Shows the tunnel mode as Normal, 802.1Q Tunnel or 802.1Q Tunnel Uplink (page 495).
802.1Q-tunnel TPID	Shows the Tag Protocol Identifier used for learning and switching packets (page 498).
Layer 2 Protocol Tunnel	Shows if L2 Protocol Tunnel is enabled for spanning tree protocol (page 503).
Broadcast Block	Shows if the broadcast packets are blocked (page 377).
Unknown Multicast Block	Shows if the unknown multicast packets are blocked (page 377).
Unknown Unicast Block	Shows if the unknown unicast packets are blocked (page 377).

show interfaces transceiver This command displays identifying information for the specified transceiver, including connector type and vendor-related parameters, as well as the temperature, voltage, bias current, transmit power, and receive power.

Syntax

show interfaces transceiver [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: SFP ports 1-52)

Default Setting

Shows all SFP interfaces.

Command Mode

Privileged Exec

Command Usage

The switch can display diagnostic information for SFP modules which support the SFF-8472 Specification for Diagnostic Monitoring Interface for Optical Transceivers. This information allows administrators to remotely diagnose problems with optical devices. This feature, referred to as Digital Diagnostic Monitoring (DDM) in the command display, provides information on transceiver parameters including temperature, supply voltage, laser bias current, laser power, received optical power, and related alarm thresholds.

Example

```
Console#show interfaces transceiver ethernet 1/25
Information of Eth 1/7
Connector Type      : LC
Fiber Type          : Multimode 50um (M5), Multimode 62.5um (M6)
Eth Compliance Codes : 1000BASE-SX
Baud Rate           : 2100 MBd
Vendor OUI          : 00-90-65
Vendor Name         : FINISAR CORP.
Vendor PN           : FTLF8519P2BNL
Vendor Rev          : A
Vendor SN           : PFS4U5F
Date Code           : 09-07-02
DDM Info
  Temperature       : 11.54 degree C
  Vcc                : 3.25 V
  Bias Current       : 7.21 mA
  TX Power           : -4.37 dBm
  RX Power           : -31.55 dBm
DDM Thresholds
-----
Low Alarm  Low Warning  High Warning  High Alarm
-----
Temperature(Celsius)  -123.00      0.00      70.00      75.00
Voltage(Volts)        3.10        3.15        3.45        3.50
Current(mA)           6.00        7.00      90.00     100.00
TxPower(dBm)          -12.00     -11.50     -9.50!     -9.00!
```

```
RxPower (dBm)          -21.50!      -21.00!      -3.50      -3.00
Console#
```

show interfaces transceiver-threshold This command Displays the alarm/warning thresholds for temperature, voltage, bias current, transmit power, and receive power. **Syntax**

Syntax

show interfaces transceiver-threshold [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: SFP ports 1-52)

Default Setting

Shows all SFP interfaces.

Command Mode

Privileged Exec

Command Usage

- ◆ The switch can display diagnostic information for SFP modules which support the SFF-8472 Specification for Diagnostic Monitoring Interface for Optical Transceivers. This information allows administrators to remotely diagnose problems with optical devices. This feature, referred to as Digital Diagnostic Monitoring (DDM) in the command display, provides information on transceiver parameters including temperature, supply voltage, laser bias current, laser power, received optical power, and related alarm thresholds.
- ◆ The DDM thresholds displayed by this command only apply to ports which have a DDM-compliant transceiver inserted.

Example

```
Console#show interfaces transceiver-threshold ethernet 1/25
Information of Eth 1/25
DDM Thresholds
```

	Low Alarm	Low Warning	High Warning	High Alarm
Temperature (Celsius)	-123.00	0.00	70.00	75.00
Voltage (Volts)	3.10	3.15	3.45	3.50
Current (mA)	6.00	7.00	90.00	100.00
TxPower (dBm)	-12.00	-11.50	-9.50	-9.00
RxPower (dBm)	-21.50	-21.00	-3.50	-3.00

```
Console#
```

Cable Diagnostics

test loop internal This command performs an internal loop back test on the specified port.

Syntax

test loop internal interface *interface*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

Command Mode

Privileged Exec

Command Usage

- ◆ Loopback testing can only be performed on a port that is not linked up. The internal loopback makes it possible to check that an interface is working properly without having to make any network connections.
- ◆ When performing an internal loopback test, packets from the specified interface are looped back into its internal PHY. Outgoing data is looped back to the receiver without actually being transmitted.

Example

```
Console#test loop internal interface ethernet 1/1
Internal loopback test: succeeded
Console#
```

show loop internal This command shows the results of a loop back test.

Syntax

show loop internal interface [*interface*]

interface

ethernet *unit/port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-52)

Command Mode

Privileged Exec

Example

```
Console#show loop internal interface ethernet 1/1
```

Port	Test Result	Last Update
-----	-----	-----
Eth 1/1	Succeeded	2013-04-15 15:26:56

```
Console#
```


Link Aggregation Commands

Ports can be statically grouped into an aggregate link (i.e., trunk) to increase the bandwidth of a network connection or to ensure fault recovery. Or you can use the Link Aggregation Control Protocol (LACP) to automatically negotiate a trunk link between this switch and another network device. For static trunks, the switches have to comply with the Cisco EtherChannel standard. For dynamic trunks, the switches have to comply with LACP. This switch supports up to 8 trunks. For example, a trunk consisting of two 1000 Mbps ports can support an aggregate bandwidth of 4 Gbps when operating at full duplex.

Table 75: Link Aggregation Commands

Command	Function	Mode
<i>Manual Configuration Commands</i>		
<code>interface port-channel</code>	Configures a trunk and enters interface configuration mode for the trunk	GC
<code>port channel load-balance</code>	Sets the load-distribution method among ports in aggregated links	GC
<code>channel-group</code>	Adds a port to a trunk	IC (Ethernet)
<i>Dynamic Configuration Commands</i>		
<code>lacp</code>	Configures LACP for the current interface	IC (Ethernet)
<code>lacp admin-key</code>	Configures a port's administration key	IC (Ethernet)
<code>lacp port-priority</code>	Configures a port's LACP port priority	IC (Ethernet)
<code>lacp system-priority</code>	Configures a port's LACP system priority	IC (Ethernet)
<code>lacp admin-key</code>	Configures an port channel's administration key	IC (Port Channel)
<code>lacp timeout</code>	Configures the timeout to wait for next LACPDU	IC (Port Channel)
<i>Trunk Status Display Commands</i>		
<code>show interfaces status port-channel</code>	Shows trunk information	NE, PE
<code>show lacp</code>	Shows LACP information	PE
<code>show port-channel load-balance</code>	Shows the load-distribution method used on aggregated links	PE

Guidelines for Creating Trunks

General Guidelines –

- ◆ Finish configuring trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- ◆ A trunk can have up to 8 ports.

- ◆ The ports at both ends of a connection must be configured as trunk ports.
- ◆ All ports in a trunk must be configured in an identical manner, including communication mode (i.e., speed and duplex mode), VLAN assignments, and CoS settings.
- ◆ Trunk groups are limited to either all 10G ports or all 40G ports. When using an LAG composed of all 10G ports, different transceiver types may be used as long as the speed of each member port is the same.
- ◆ All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN via the specified port-channel.
- ◆ STP, VLAN, and IGMP settings can only be made for the entire trunk via the specified port-channel.

Dynamically Creating a Port Channel –

Ports assigned to a common port channel must meet the following criteria:

- ◆ Ports must have the same LACP system priority.
- ◆ Ports must have the same port admin key (Ethernet Interface).
- ◆ If the port channel admin key ([lACP admin key](#) - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key ([lACP admin key](#) - Ethernet Interface) used by the interfaces that joined the group.
- ◆ However, if the port channel admin key is set, then the port admin key must be set to the same value for a port to be allowed to join a channel group.
- ◆ If a link goes down, LACP port priority is used to select the backup link.

Manual Configuration Commands

port channel load-balance This command sets the load-distribution method among ports in aggregated links (for both static and dynamic trunks). Use the **no** form to restore the default setting.

Syntax

port channel load-balance {dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac}

no port channel load-balance

dst-ip - Load balancing based on destination IP address.

dst-mac - Load balancing based on destination MAC address.

src-dst-ip - Load balancing based on source and destination IP address.

src-dst-mac - Load balancing based on source and destination MAC address.

src-ip - Load balancing based on source IP address.

src-mac - Load balancing based on source MAC address.

Default Setting

src-dst-ip

Command Mode

Global Configuration

Command Usage

- ◆ This command applies to all static and dynamic trunks on the switch.
- ◆ To ensure that the switch traffic load is distributed evenly across all links in a trunk, select the source and destination addresses used in the load-balance calculation to provide the best result for trunk connections:
 - **dst-ip:** All traffic with the same destination IP address is output on the same link in a trunk. This mode works best for switch-to-router trunk links where traffic through the switch is destined for many different hosts. Do not use this mode for switch-to-server trunk links where the destination IP address is the same for all traffic.
 - **dst-mac:** All traffic with the same destination MAC address is output on the same link in a trunk. This mode works best for switch-to-switch trunk links where traffic through the switch is destined for many different hosts. Do not use this mode for switch-to-router trunk links where the destination MAC address is the same for all traffic.
 - **src-dst-ip:** All traffic with the same source and destination IP address is output on the same link in a trunk. This mode works best for switch-to-router trunk links where traffic through the switch is received from and destined for many different hosts.
 - **src-dst-mac:** All traffic with the same source and destination MAC address is output on the same link in a trunk. This mode works best for switch-to-switch trunk links where traffic through the switch is received from and destined for many different hosts.
 - **src-ip:** All traffic with the same source IP address is output on the same link in a trunk. This mode works best for switch-to-router or switch-to-server trunk links where traffic through the switch is received from many different hosts.
 - **src-mac:** All traffic with the same source MAC address is output on the same link in a trunk. This mode works best for switch-to-switch trunk links where traffic through the switch is received from many different hosts.

Example

```
Console(config)#port-channel load-balance dst-ip
Console(config)#
```

channel-group This command adds a port to a trunk. Use the **no** form to remove a port from a trunk.

Syntax

channel-group *channel-id*

no channel-group

channel-id - Trunk index (Range: 1-8)

Default Setting

The current port will be added to this trunk.

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ When configuring static trunks, the switches must comply with the Cisco EtherChannel standard.
- ◆ Use **no channel-group** to remove a port group from a trunk.
- ◆ Use **no interface port-channel** to remove a trunk from the switch.

Example

The following example creates trunk 1 and then adds port 10-12:

```
Console(config)#interface port-channel 1
Console(config-if)#exit
Console(config)#interface ethernet 1/10-12
Console(config-if)#channel-group 1
Console(config-if)#
```

Dynamic Configuration Commands

lacp This command enables 802.3ad Link Aggregation Control Protocol (LACP) for the current interface. Use the **no** form to disable it.

Syntax

[no] lacp

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ The ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.
- ◆ A trunk formed with another switch using LACP will automatically be assigned the next available port-channel ID.
- ◆ If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.
- ◆ If more than eight ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.

Example

The following shows LACP enabled on ports 1-3. Because LACP has also been enabled on the ports at the other end of the links, the `show interfaces status port-channel 1` command shows that Trunk1 has been established.

```
Console(config)#interface ethernet 1/1-3
Console(config-if)#lACP
Console(config-if)#end
Console#show interfaces status port-channel 1
Information of Trunk 1
Basic Information:
  Port Type           : 1000Base SFP
  MAC Address         : 12-34-12-34-12-3F
Configuration:
  Name                :
  Port Admin          : Up
  Speed-duplex        : 1000full
  Capabilities        : 1000full
  Broadcast Storm     : Enabled
  Broadcast Storm Limit : 262143 packets/second
  Multicast Storm     : Disabled
  Multicast Storm Limit : 262143 Kbits/second
  Unknown Unicast Storm : Disabled
  Unknown Unicast Storm Limit : 262143 Kbits/second
  Flow Control        : Disabled
  VLAN Trunking       : Disabled
  MAC Learning        : Enabled
  MTU                 : 1518
Current status:
  Created By          : LACP
  Link Status         : Up
  Port Operation Status : Up
  Operation speed-duplex : 1000full
  Up Time             : 0w 0d 0h 14s (14 seconds)
  Flow control Type    : None
  Max Frame Size       : 1518 bytes (1522 bytes for tagged frames)
  MAC Learning Status  : Enabled
  Member Ports        : Eth1/1, Eth1/2, Eth1/3,
  Active Member Ports  : Eth1/1
Console#
```

lacp admin-key (Ethernet Interface) This command configures a port's LACP administration key. Use the **no** form to restore the default setting.

Syntax

lacp {actor | partner} admin-key *key*

no lacp {actor | partner} admin-key

actor - The local side an aggregate link.

partner - The remote side of an aggregate link.

key - The port admin key must be set to the same value for ports that belong to the same link aggregation group (LAG). (Range: 0-65535)

Default Setting

Actor: 1, Partner: 0

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ Ports are only allowed to join the same LAG if (1) the LACP system priority matches, (2) the LACP port admin key matches, and (3) the LACP port channel key matches (if configured).
- ◆ If the port channel admin key (**lacp admin key** - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (**lacp admin key** - Ethernet Interface) used by the interfaces that joined the group.
- ◆ Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor admin-key 120
Console(config-if)#
```

lacp port-priority This command configures LACP port priority. Use the **no** form to restore the default setting.

Syntax

lacp {actor | partner} port-priority *priority*

no lacp {actor | partner} port-priority

actor - The local side an aggregate link.

partner - The remote side of an aggregate link.

priority - LACP port priority is used to select a backup link. (Range: 0-65535)

Default Setting

32768

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ Setting a lower value indicates a higher effective priority.
- ◆ If an active port link goes down, the backup port with the highest priority is selected to replace the downed link. However, if two or more ports have the same LACP port priority, the port with the lowest physical port number will be selected as the backup port.
- ◆ If an LAG already exists with the maximum number of allowed port members, and LACP is subsequently enabled on another port using a higher priority than an existing member, the newly configured port will replace an existing port member that has a lower priority.
- ◆ Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor port-priority 128
```

lacp system-priority This command configures a port's LACP system priority. Use the **no** form to restore the default setting.

Syntax

lacp {actor | partner} system-priority *priority*

no lacp {actor | partner} system-priority

actor - The local side an aggregate link.

partner - The remote side of an aggregate link.

priority - This priority is used to determine link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations. (Range: 0-65535)

Default Setting

32768

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ Port must be configured with the same system priority to join the same LAG.
- ◆ System priority is combined with the switch's MAC address to form the LAG identifier. This identifier is used to indicate a specific LAG during LACP negotiations with other systems.
- ◆ Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#lACP actor system-priority 3
Console(config-if)#
```

lACP admin-key (Port Channel) This command configures a port channel's LACP administration key string. Use the **no** form to restore the default setting.

Syntax

lACP admin-key *key*

no lACP admin-key

key - The port channel admin key is used to identify a specific link aggregation group (LAG) during local LACP setup on this switch.
(Range: 0-65535)

Default Setting

0

Command Mode

Interface Configuration (Port Channel)

Command Usage

- ◆ Ports are only allowed to join the same LAG if (1) the LACP system priority matches, (2) the LACP port admin key matches, and (3) the LACP port channel key matches (if configured).
- ◆ If the port channel admin key (**lACP admin key** - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the

same value as the port admin key ([lacp admin key](#) - Ethernet Interface) used by the interfaces that joined the group. Note that when the LAG is no longer used, the port channel admin key is reset to 0.

Example

```
Console(config)#interface port-channel 1
Console(config-if)#lacp admin-key 3
Console(config-if)#
```

lacp timeout This command configures the timeout to wait for the next LACP data unit (LACPDU). Use the no form to restore the default setting.

Syntax

lacp timeout {long | short}

no lacp timeout

long - Specifies a slow timeout of 90 seconds.

short - Specifies a fast timeout of 3 seconds.

Default Setting

long

Command Mode

Interface Configuration (Port Channel)

Command Usage

- ◆ The timeout configured by this command is set in the LACP timeout bit of the Actor State field in transmitted LACPDU. When the partner switch receives an LACPDU set with a short timeout from the actor switch, the partner adjusts the transmit LACPDU interval to 1 second. When it receives an LACPDU set with a long timeout from the actor, it adjusts the transmit LACPDU interval to 30 seconds.
- ◆ If the actor does not receive an LACPDU from its partner before the configured timeout expires, the partner port information will be deleted from the LACP group.
- ◆ When a dynamic port-channel member leaves a port-channel, the default timeout value will be restored on that port.
- ◆ When a dynamic port-channel is torn down, the configured timeout value will be retained. When the dynamic port-channel is constructed again, that timeout value will be used.

Example

```
Console(config)#interface port-channel 1
Console(config-if)#lACP timeout short
Console(config-if)#
```

Trunk Status Display Commands

show lacp This command displays LACP information.

Syntax

show lacp [*port-channel*] {**counters** | **internal** | **neighbors** | **sys-id**}

port-channel - Local identifier for a link aggregation group. (Range: 1-8)

counters - Statistics for LACP protocol messages.

internal - Configuration settings and operational state for local side.

neighbors - Configuration settings and operational state for remote side.

sys-id - Summary of system priority and MAC address for all channel groups.

Default Setting

Port Channel: all

Command Mode

Privileged Exec

Example

```
Console#show lacp 1 counters
Port Channel: 1
-----
Eth 1/ 2
-----
LACPDU Sent      : 12
LACPDU Received  : 6
Marker Sent      : 0
Marker Received   : 0
LACPDU Unknown Pkts : 0
LACPDU Illegal Pkts : 0
:
```

Table 76: show lacp counters - display description

Field	Description
LACPDU Sent	Number of valid LACPDU transmitted from this channel group.
LACPDU Received	Number of valid LACPDU received on this channel group.
Marker Sent	Number of valid Marker PDU transmitted from this channel group.
Marker Received	Number of valid Marker PDU received by this channel group.

Table 76: show lacp counters - display description (Continued)

Field	Description
LACPDUs Unknown Pkts	Number of frames received that either (1) Carry the Slow Protocols Ethernet Type value, but contain an unknown PDU, or (2) are addressed to the Slow Protocols group MAC Address, but do not carry the Slow Protocols Ethernet Type.
LACPDUs Illegal Pkts	Number of frames that carry the Slow Protocols Ethernet Type value, but contain a badly formed PDU or an illegal value of Protocol Subtype.

```

Console#show lacp 1 internal
Port Channel : 1
-----
Oper Key   : 3
Admin Key  : 0
Eth 1/ 1

-----
LACPDUs Internal      : 30 seconds
LACP System Priority  : 32768
LACP Port Priority    : 32768
Admin Key             : 3
Oper Key              : 3
Admin State           : defaulted, aggregation, long timeout, LACP-activity
Oper State            : distributing, collecting, synchronization,
                        aggregation, long timeout, LACP-activity
:

```

Table 77: show lacp internal - display description

Field	Description
Oper Key	Current operational value of the key for the aggregation port.
Admin Key	Current administrative value of the key for the aggregation port.
LACPDUs Internal	Number of seconds before invalidating received LACPDU information.
LACP System Priority	LACP system priority assigned to this port channel.
LACP Port Priority	LACP port priority assigned to this interface within the channel group.

Table 77: show lacp internal - display description (Continued)

Field	Description
Admin State, Oper State	<p>Administrative or operational values of the actor's state parameters:</p> <ul style="list-style-type: none"> Expired – The actor's receive machine is in the expired state; Defaulted – The actor's receive machine is using defaulted operational partner information, administratively configured for the partner. Distributing – If false, distribution of outgoing frames on this link is disabled; i.e., distribution is currently disabled and is not expected to be enabled in the absence of administrative changes or changes in received protocol information. Collecting – Collection of incoming frames on this link is enabled; i.e., collection is currently enabled and is not expected to be disabled in the absence of administrative changes or changes in received protocol information. Synchronization – The System considers this link to be IN_SYNC; i.e., it has been allocated to the correct Link Aggregation Group, the group has been associated with a compatible Aggregator, and the identity of the Link Aggregation Group is consistent with the System ID and operational Key information transmitted. Aggregation – The system considers this link to be aggregatable; i.e., a potential candidate for aggregation. Long timeout – Periodic transmission of LACPDUs uses a slow transmission rate. LACP-Activity – Activity control value with regard to this link. (0: Passive; 1: Active)

```

Console#show lacp 1 neighbors
Port Channel 1 neighbors
-----
Eth 1/ 1
-----
Partner Admin System ID   : 32768, 00-00-00-00-00-00
Partner Oper System ID   : 32768, 00-12-CF-61-24-2F
Partner Admin Port Number : 1
Partner Oper Port Number  : 1
Port Admin Priority       : 32768
Port Oper Priority        : 32768
Admin Key                 : 0
Oper Key                  : 3
Admin State:              defaulted, distributing, collecting,
                           synchronization, long timeout,
Oper State:               distributing, collecting, synchronization,
                           aggregation, long timeout, LACP-activity
:

```

Table 78: show lacp neighbors - display description

Field	Description
Partner Admin System ID	LAG partner's system ID assigned by the user.
Partner Oper System ID	LAG partner's system ID assigned by the LACP protocol.
Partner Admin Port Number	Current administrative value of the port number for the protocol Partner.
Partner Oper Port Number	Operational port number assigned to this aggregation port by the port's protocol partner.

Table 78: show lacp neighbors - display description (Continued)

Field	Description
Port Admin Priority	Current administrative value of the port priority for the protocol partner.
Port Oper Priority	Priority value assigned to this aggregation port by the partner.
Admin Key	Current administrative value of the Key for the protocol partner.
Oper Key	Current operational value of the Key for the protocol partner.
Admin State	Administrative values of the partner's state parameters. (See preceding table.)
Oper State	Operational values of the partner's state parameters. (See preceding table.)

```

Console#show lacp sysid
Port Channel      System Priority    System MAC Address
-----
                1          32768      00-30-F1-8F-2C-A7
                2          32768      00-30-F1-8F-2C-A7
                3          32768      00-30-F1-8F-2C-A7
                4          32768      00-30-F1-8F-2C-A7
                5          32768      00-30-F1-8F-2C-A7
                6          32768      00-30-F1-8F-2C-A7
                7          32768      00-30-F1-D4-73-A0
                8          32768      00-30-F1-D4-73-A0
                9          32768      00-30-F1-D4-73-A0
               10          32768      00-30-F1-D4-73-A0
               11          32768      00-30-F1-D4-73-A0
               12          32768      00-30-F1-D4-73-A0
               :

```

Table 79: show lacp sysid - display description

Field	Description
Channel group	A link aggregation group configured on this switch.
System Priority*	LACP system priority for this channel group.
System MAC Address*	System MAC address.

* The LACP system priority and system MAC address are concatenated to form the LAG system ID.

show port-channel load-balance This command shows the load-distribution method used on aggregated links.

Command Mode
Privileged Exec

Example

```

Console#show port-channel load-balance
Trunk Load Balance Mode: Destination IP address
Console#

```


Port Mirroring Commands

Data can be mirrored from a local port on the same switch or from a remote port on another switch for analysis at the target port using software monitoring tools or a hardware probe. This switch supports the following mirroring modes.

Table 80: Port Mirroring Commands

Command	Function
Local Port Mirroring	Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port
RSPAN Mirroring	Mirrors data from remote switches over a dedicated VLAN

Local Port Mirroring Commands

This section describes how to mirror traffic from a source port to a target port.

Table 81: Mirror Port Commands

Command	Function	Mode
port monitor	Configures a mirror session	IC
show port monitor	Shows the configuration for a mirror port	PE

port monitor This command configures a mirror session. Use the **no** form to clear a mirror session.

Syntax

port monitor *interface* [**rx** | **tx** | **both**]

no port monitor *interface*

interface - **ethernet** *unit/port* (source port)

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

rx - Mirror received packets.

tx - Mirror transmitted packets.

both - Mirror both received and transmitted packets.

Default Setting

- ◆ No mirror session is defined.
- ◆ When enabled for an interface, default mirroring is for both received and transmitted packets.
- ◆ When enabled for a VLAN or a MAC address, mirroring is restricted to received packets.

Command Mode

Interface Configuration (Ethernet, destination port)

Command Usage

- ◆ You can mirror traffic from any source port to a destination port for real-time analysis. You can then attach a logic analyzer or RMON probe to the destination port and study the traffic crossing the source port in a completely unobtrusive manner.
- ◆ Set the destination port by specifying an Ethernet interface with the [interface](#) configuration command, and then use the **port monitor** command to specify the source of the traffic to mirror.
- ◆ When mirroring traffic from a port, the mirror port and monitor port speeds should match, otherwise traffic may be dropped from the monitor port. When mirroring traffic from a VLAN, traffic may also be dropped under heavy loads.
- ◆ Note that Spanning Tree BPDU packets are not mirrored to the target port.
- ◆ You can create multiple mirror sessions, but all sessions must share the same destination port.
- ◆ The destination port cannot be a trunk or trunk member port.

Example

The following example configures the switch to mirror all packets from port 6 to 5:

```
Console(config)#interface ethernet 1/5
Console(config-if)#port monitor ethernet 1/6 both
Console(config-if)#
```

show port monitor This command displays mirror information.

Syntax

show port monitor [*interface*]

interface - **ethernet** *unit/port* (source port)

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

Default Setting

Shows all sessions.

Command Mode

Privileged Exec

Command Usage

This command displays the currently configured source port, destination port, and mirror mode (i.e., RX, TX, RX/TX).

Example

The following shows mirroring configured from port 6 to port 5:

```
Console(config)#interface ethernet 1/5
Console(config-if)#port monitor ethernet 1/6
Console(config-if)#end
Console#show port monitor
Port Mirroring
-----
Destination Port (listen port):Eth1/5
Source Port (monitored port) :Eth1/6
Mode                        :RX/TX
Console#
```

RSPAN Mirroring Commands

Remote Switched Port Analyzer (RSPAN) allows you to mirror traffic from remote switches for analysis on a local destination port.

Table 82: RSPAN Commands

Command	Function	Mode
<code>vlan rspan</code>	Creates a VLAN dedicated to carrying RSPAN traffic	VC
<code>rspan source</code>	Specifies the source port and traffic type to be mirrored	GC
<code>rspan destination</code>	Specifies the destination port to monitor the mirrored traffic	GC
<code>rspan remote vlan</code>	Specifies the RSPAN VLAN, switch role (source, intermediate or destination), and the uplink ports	GC
<code>no rspan session</code>	Deletes a configured RSPAN session	GC
<code>show rspan</code>	Displays the configuration settings for an RSPAN session	PE

Configuration Guidelines

Take the following steps to configure an RSPAN session:

1. Use the `vlan rspan` command to configure a VLAN to use for RSPAN. (Default VLAN 1 and switch cluster VLAN 4093 are prohibited.)
2. Use the `rspan source` command to specify the interfaces and the traffic type (RX, TX or both) to be monitored.
3. Use the `rspan destination` command to specify the destination port for the traffic mirrored by an RSPAN session.
4. Use the `rspan remote vlan` command to specify the VLAN to be used for an RSPAN session, to specify the switch's role as a source, intermediate relay, or destination of the mirrored traffic, and to configure the uplink ports designated to carry this traffic.

RSPAN Limitations

The following limitations apply to the use of RSPAN on this switch:

- ◆ *RSPAN Ports* – Only ports can be configured as an RSPAN source, destination, or uplink; static and dynamic trunks are not allowed. A port can only be configured as one type of RSPAN interface – source, destination, or uplink. Also, note that the source port and destination port cannot be configured on the same switch.
- ◆ *Local/Remote Mirror* – The destination of a local mirror session (created with the `port monitor` command) cannot be used as the destination for RSPAN traffic.
Only two mirror sessions are allowed. Both sessions can be allocated to remote mirroring, unless local mirroring is enabled (which is limited to a single session).
- ◆ *Spanning Tree* – If the spanning tree is disabled, BPDUs will not be flooded onto the RSPAN VLAN.
MAC address learning is not supported on RSPAN uplink ports when RSPAN is enabled on the switch. Therefore, even if spanning tree is enabled after RSPAN has been configured, MAC address learning will still not be re-started on the RSPAN uplink ports.
- ◆ *IEEE 802.1X* – RSPAN and 802.1X are mutually exclusive functions. When 802.1X is enabled globally, RSPAN uplink ports cannot be configured, even though RSPAN source and destination ports can still be configured. When RSPAN uplink ports are enabled on the switch, 802.1X cannot be enabled globally.
RSPAN uplink ports cannot be configured to use IEEE 802.1X Port Authentication, but RSPAN source ports and destination ports can be configured to use it

- ◆ *Port Security* – If port security is enabled on any port, that port cannot be set as an RSPAN uplink port, even though it can still be configured as an RSPAN source or destination port. Also, when a port is configured as an RSPAN uplink port, port security cannot be enabled on that port.

rspan source Use this command to specify the source port and traffic type to be mirrored remotely. Use the **no** form to disable RSPAN on the specified port, or with a traffic type keyword to disable mirroring for the specified type.

Syntax

[no] rspan session *session-id* source interface *interface* [rx | tx | both]

session-id – A number identifying this RSPAN session. (Range: 1-2)

Only two mirror sessions are allowed, including both local and remote mirroring. If local mirroring is enabled with the **port monitor** command, then there is only one session available for RSPAN.

interface

ethernet *unit/port-list*

unit - Unit identifier. (Range: 1)

port-list - One or more source ports. Use a hyphen to indicate a consecutive list of ports or a comma between non-consecutive ports. (Range: 1-52)

rx - Mirror received packets.

tx - Mirror transmitted packets.

both - Mirror both received and transmitted packets.

Default Setting

Both TX and RX traffic is mirrored

Command Mode

Global Configuration

Command Usage

- ◆ One or more source ports can be assigned to the same RSPAN session, either on the same switch or on different switches.
- ◆ Only ports can be configured as an RSPAN source – static and dynamic trunks are not allowed.
- ◆ The source port and destination port cannot be configured on the same switch.

Example

The following example configures the switch to mirror received packets from port 2 and 3:

```
Console(config)#rspan session 1 source interface ethernet 1/2 rx
Console(config)#rspan session 1 source interface ethernet 1/3 rx
Console(config)#
```

rspan destination Use this command to specify the destination port to monitor the mirrored traffic. Use the **no** form to disable RSPAN on the specified port.

Syntax

rspan session *session-id* **destination interface** *interface* [**tagged** | **untagged**]

no rspan session *session-id* **destination interface** *interface*

session-id – A number identifying this RSPAN session. (Range: 1-2)

Only two mirror sessions are allowed, including both local and remote mirroring. If local mirroring is enabled with the **port monitor** command, then there is only one session available for RSPAN.

interface - **ethernet** *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

tagged - Traffic exiting the destination port carries the RSPAN VLAN tag.

untagged - Traffic exiting the destination port is untagged.

Default Setting

Traffic exiting the destination port is untagged.

Command Mode

Global Configuration

Command Usage

- ◆ Only one destination port can be configured on the same switch per session, but a destination port can be configured on more than one switch for the same session.
- ◆ Only ports can be configured as an RSPAN destination – static and dynamic trunks are not allowed.
- ◆ The source port and destination port cannot be configured on the same switch.
- ◆ A destination port can still send and receive switched traffic, and participate in any Layer 2 protocols to which it has been assigned.

Example

The following example configures port 4 to receive mirrored RSPAN traffic:

```
Console(config)#rspan session 1 destination interface ethernet 1/4
Console(config)#
```

rspan remote vlan Use this command to specify the RSPAN VLAN, switch role (source, intermediate or destination), and the uplink ports. Use the **no** form to disable the RSPAN on the specified VLAN.

Syntax

[no] rspan session *session-id* **remote vlan** *vlan-id*
{source | intermediate | destination} **uplink** *interface*

session-id – A number identifying this RSPAN session. (Range: 1-2)

Only two mirror sessions are allowed, including both local and remote mirroring. If local mirroring is enabled with the [port monitor](#) command, then there is only one session available for RSPAN.

vlan-id - ID of configured RSPAN VLAN. (Range: 2-4092)

Use the [vlan rspan](#) command to reserve a VLAN for RSPAN mirroring before enabling RSPAN with this command.

source - Specifies this device as the source of remotely mirrored traffic.

intermediate - Specifies this device as an intermediate switch, transparently passing mirrored traffic from one or more sources to one or more destinations.

destination - Specifies this device as a switch configured with a destination port which is to receive mirrored traffic for this session.

uplink - A port configured to receive or transmit remotely mirrored traffic.

interface - **ethernet** *unit/port*

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ Only one uplink port can be configured on a source switch, but there is no limitation on the number of uplink ports configured on an intermediate or destination switch.

- ◆ Only destination and uplink ports will be assigned by the switch as members of this VLAN. Ports cannot be manually assigned to an RSPAN VLAN with the `switchport allowed vlan` command. Nor can GVRP dynamically add port members to an RSPAN VLAN. Also, note that the `show vlan` command will not display any members for an RSPAN VLAN, but will only show configured RSPAN VLAN identifiers.

Example

The following example enables RSPAN on VLAN 2, specifies this device as an RSPAN destination switch, and the uplink interface as port 3:

```
Console(config)#rspan session 1 remote vlan 2 destination uplink ethernet 1/3
Console(config)#
```

no rspan session Use this command to delete a configured RSPAN session.

Syntax

no rspan session *session-id*

session-id – A number identifying this RSPAN session. (Range: 1-2)

Only two mirror sessions are allowed, including both local and remote mirroring. If local mirroring is enabled with the `port monitor` command, then there is only one session available for RSPAN.

Command Mode

Global Configuration

Command Usage

The **no rspan session** command must be used to disable an RSPAN VLAN before it can be deleted from the VLAN database (see the `vlan` command).

Example

```
Console(config)#no rspan session 1
Console(config)#
```

show rspan Use this command to displays the configuration settings for an RSPAN session.

Syntax

show rspan session [*session-id*]

session-id – A number identifying this RSPAN session. (Range: 1-2)

Only two mirror sessions are allowed, including both local and remote mirroring. If local mirroring is enabled with the `port monitor` command, then there is only one session available for RSPAN.

Command Mode
Privileged Exec

Example

```
Console#show rspan session
RSPAN Session ID           : 1
Source Ports (mirrored ports) : None
  RX Only                  : None
  TX Only                  : None
  BOTH                     : None
Destination Port (monitor port) : Eth 1/2
Destination Tagged Mode      : Untagged
Switch Role                  : Destination
RSPAN VLAN                   : 2
RSPAN Uplink Ports           : Eth 1/3
Operation Status              : Up
Console#
```


Congestion Control Commands

The switch can set the maximum upload or download data transfer rate for any port. It can control traffic storms by setting a maximum threshold for broadcast traffic or multicast traffic. It can also set bounding thresholds for broadcast and multicast storms which can be used to automatically trigger rate limits or to shut down a port.

Table 83: Congestion Control Commands

Command Group	Function
Rate Limiting	Sets the input and output rate limits for a port.
Storm Control	Sets the traffic storm threshold for each port.
Automatic Traffic Control	Sets thresholds for broadcast and multicast storms which can be used to trigger configured rate limits or to shut down a port.

Rate Limit Commands

Rate limit commands allow the network manager to control the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or trunks. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped.

Table 84: Rate Limit Commands

Command	Function	Mode
rate-limit	Configures the maximum input or output rate for an interface	IC

rate-limit This command defines the rate limit for a specific interface. Use this command without specifying a rate to restore the default rate. Use the **no** form to restore the default status of disabled.

Syntax

rate-limit {input | output} [*rate*]

no rate-limit {input | output}

input – Input rate for specified interface

output – Output rate for specified interface

rate – Maximum value in Kbps.

(Range: 64 - 10,000,000 Kbits per second for 10G Ethernet ports;
64 - 40,000,000 Kbits per second for 40G Ethernet ports)

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

Using both rate limiting and storm control on the same interface may lead to unexpected results. For example, suppose broadcast storm control is set to 50,000 Kbps by the command "switchport broadcast packet-rate 50000," and the rate limit is set to 1,000,000 Kbps by the command "rate-limit input 2,000,000" on a 10G Ethernet port. Since 2,000,000 Kbps is 1/5 of line speed, the received rate will actually be 10,000 Kbps, or 1/5 of the 50,000 Kbps limit set by the storm control command. It is therefore not advisable to use both of these commands on the same interface.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#rate-limit input 64
Console(config-if)#
```

Related Command

[show interfaces switchport \(394\)](#)

Storm Control Commands

Storm control commands can be used to configure broadcast, multicast, and unknown unicast storm control thresholds. Traffic storms may occur when a device on your network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much traffic on your network, performance can be severely degraded or everything can come to complete halt.

You can protect your network from traffic storms by setting a threshold for broadcast, multicast or unknown unicast traffic. Any packets exceeding the specified threshold will then be dropped.

Table 85: Rate Limit Commands

Command	Function	Mode
<code>switchport packet-rate</code> *	Configures broadcast, multicast, and unknown unicast storm control thresholds	IC
<code>show interfaces switchport</code>	Displays the administrative and operational status of an interface	NE, PE

* Enabling hardware-level storm control with this command on a port will disable software-level automatic storm control on the same port if configured by the `auto-traffic-control` command.

switchport packet-rate This command configures broadcast, multicast and unknown unicast storm control. Use the **no** form to restore the default setting.

Syntax

switchport {broadcast | multicast | unicast} packet-rate rate

no switchport {broadcast | multicast | unicast}

broadcast - Specifies storm control for broadcast traffic.

multicast - Specifies storm control for multicast traffic.

unicast - Specifies storm control for unknown unicast traffic.

rate - Threshold level as a rate; i.e., kilobits per second.
(Range: 500-14880000 pps)

Default Setting

Broadcast Storm Control: Enabled, 500 pps

Multicast Storm Control: Disabled

Unknown Unicast Storm Control: Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ When traffic exceeds the threshold specified for broadcast and multicast or unknown unicast traffic, packets exceeding the threshold are dropped until the rate falls back down beneath the threshold.
- ◆ Traffic storms can be controlled at the hardware level using this command or at the software level using the [auto-traffic-control](#) command. However, only one of these control types can be applied to a port. Enabling hardware-level storm control on a port will disable automatic storm control on that port.
- ◆ The rate limits set by this command are also used by automatic storm control when the control response is set to rate limiting by the [auto-traffic-control action](#) command.
- ◆ Using both rate limiting and storm control on the same interface may lead to unexpected results. For example, suppose broadcast storm control is set to 5,000 pps by the command "switchport broadcast packet-rate 5000" and the rate limit is set to 2 Gbps by the command "rate-limit input 2000" on a 10G port. Since 2 Gbps is 1/5 of line speed (10 Gbps), the received rate will actually be 1,000 pps, or 1/5 of the 5,000 pps limit set by the storm control command. It is therefore not advisable to use both of these commands on the same interface.

Example

The following shows how to configure broadcast storm control at 600 kilobits per second:

```
Console(config)#interface ethernet 1/5
Console(config-if)#switchport broadcast packet-rate 600
Console(config-if)#
```

Automatic Traffic Control Commands

Automatic Traffic Control (ATC) configures bounding thresholds for broadcast and multicast storms which can be used to trigger configured rate limits or to shut down a port.

Table 86: ATC Commands

Command	Function	Mode
<i>Threshold Commands</i>		
auto-traffic-control apply-timer	Sets the time at which to apply the control response after ingress traffic has exceeded the upper threshold	GC
auto-traffic-control release-timer	Sets the time at which to release the control response after ingress traffic has fallen beneath the lower threshold	GC
auto-traffic-control*	Enables automatic traffic control for broadcast or multicast storms	IC (Port)

Table 86: ATC Commands (Continued)

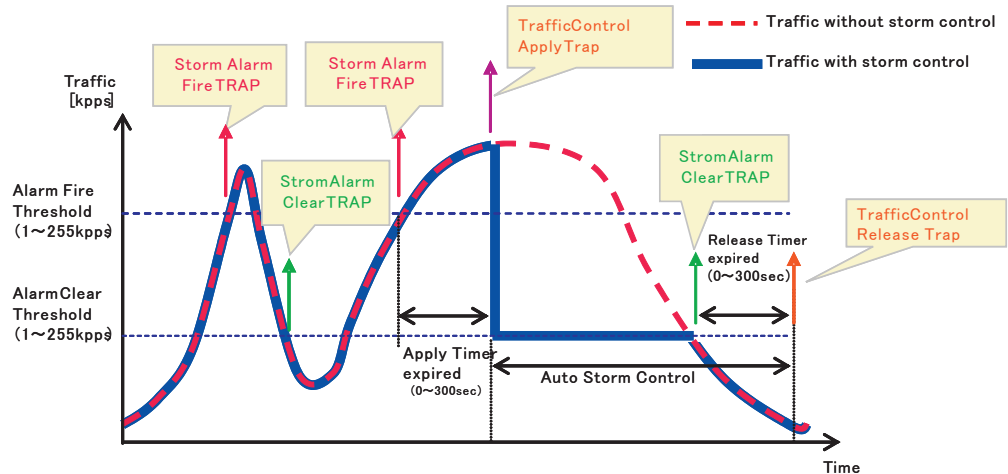
Command	Function	Mode
<code>auto-traffic-control action</code>	Sets the control action to limit ingress traffic or shut down the offending port	IC (Port)
<code>auto-traffic-control alarm-clear-threshold</code>	Sets the lower threshold for ingress traffic beneath which a cleared storm control trap is sent	IC (Port)
<code>auto-traffic-control alarm-fire-threshold</code>	Sets the upper threshold for ingress traffic beyond which a storm control response is triggered after the apply timer expires	IC (Port)
<code>auto-traffic-control auto-control-release</code>	Automatically releases a control response	IC (Port)
<code>auto-traffic-control control-release</code>	Manually releases a control response	IC (Port)
<i>SNMP Trap Commands</i>		
<code>snmp-server enable port-traps atc broadcast-alarm-clear</code>	Sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered	IC (Port)
<code>snmp-server enable port-traps atc broadcast-alarm-fire</code>	Sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control	IC (Port)
<code>snmp-server enable port-traps atc broadcast-control-apply</code>	Sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control and the apply timer expires	IC (Port)
<code>snmp-server enable port-traps atc broadcast-control-release</code>	Sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires	IC (Port)
<code>snmp-server enable port-traps atc multicast-alarm-clear</code>	Sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered	IC (Port)
<code>snmp-server enable port-traps atc multicast-alarm-fire</code>	Sends a trap when multicast traffic exceeds the upper threshold for automatic storm control	IC (Port)
<code>snmp-server enable port-traps atc multicast-control-apply</code>	Sends a trap when multicast traffic exceeds the upper threshold for automatic storm control and the apply timer expires	IC (Port)
<code>snmp-server enable port-traps atc multicast-control-release</code>	Sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires	IC (Port)
<i>ATC Display Commands</i>		
<code>show auto-traffic-control</code>	Shows global configuration settings for automatic storm control	PE
<code>show auto-traffic-control interface</code>	Shows interface configuration settings and storm control status for the specified port	PE

* Enabling automatic storm control on a port will disable hardware-level storm control on the same port if configured by the `switchport packet-rate` command.

Usage Guidelines

ATC includes storm control for broadcast or multicast traffic. The control response for either of these traffic types is the same, as shown in the following diagrams.

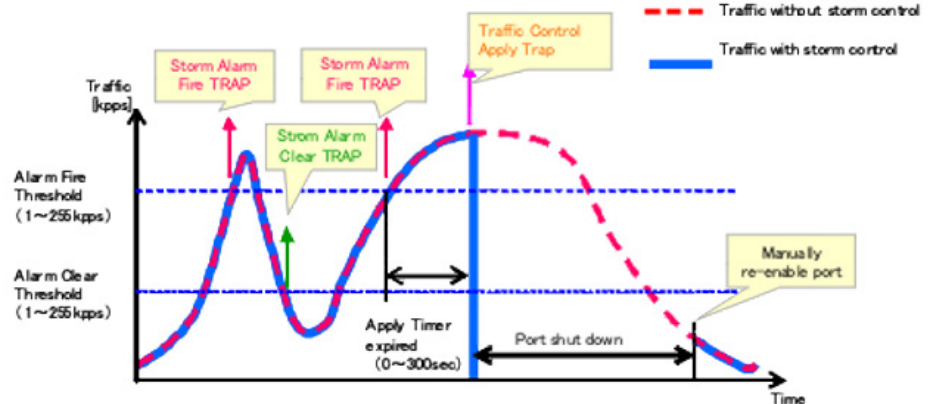
Figure 1: Storm Control by Limiting the Traffic Rate



The key elements of this diagram are described below:

- ◆ **Alarm Fire Threshold** – The highest acceptable traffic rate. When ingress traffic exceeds the threshold, ATC sends a Storm Alarm Fire Trap and logs it.
- ◆ When traffic exceeds the alarm fire threshold and the apply timer expires, a traffic control response is applied, and a Traffic Control Apply Trap is sent and logged.
- ◆ **Alarm Clear Threshold** – The lower threshold beneath which a control response can be automatically terminated after the release timer expires. When ingress traffic falls below this threshold, ATC sends a Storm Alarm Clear Trap and logs it.
- ◆ When traffic falls below the alarm clear threshold after the release timer expires, traffic control (for rate limiting) will be stopped and a Traffic Control Release Trap sent and logged. Note that if the control action has shut down a port, it can only be manually re-enabled using the [auto-traffic-control control-release](#) command).
- ◆ The traffic control response of rate limiting can be released automatically or manually. The control response of shutting down a port can only be released manually.

Figure 2: Storm Control by Shutting Down a Port



The key elements of this diagram are the same as that described in the preceding diagram, except that automatic release of the control response is not provided. When traffic control is applied, you must manually re-enable the port.

Functional Limitations

Automatic storm control is a software level control function. Traffic storms can also be controlled at the hardware level using the [switchport packet-rate](#) command. However, only one of these control types can be applied to a port. Enabling automatic storm control on a port will disable hardware-level storm control on that port.

Threshold Commands

auto-traffic-control apply-timer This command sets the time at which to apply the control response after ingress traffic has exceeded the upper threshold. Use the **no** form to restore the default setting.

Syntax

auto-traffic-control {broadcast | multicast} apply-timer seconds

no auto-traffic-control {broadcast | multicast} apply-timer

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

seconds - The interval after the upper threshold has been exceeded at which to apply the control response. (Range: 1-300 seconds)

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

After the apply timer expires, a control action may be triggered as specified by the [auto-traffic-control action](#) command and a trap message sent as specified by the [snmp-server enable port-traps atc broadcast-control-apply](#) command or [snmp-server enable port-traps atc multicast-control-apply](#) command.

Example

This example sets the apply timer to 200 seconds for all ports.

```
Console(config)#auto-traffic-control broadcast apply-timer 200
Console(config)#
```

auto-traffic-control release-timer

This command sets the time at which to release the control response after ingress traffic has fallen beneath the lower threshold. Use the **no** form to restore the default setting.

Syntax

auto-traffic-control {broadcast | multicast} release-timer *seconds*

no auto-traffic-control {broadcast | multicast} release-timer

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

seconds - The time at which to release the control response after ingress traffic has fallen beneath the lower threshold. (Range: 1-900 seconds)

Default Setting

900 seconds

Command Mode

Global Configuration

Command Usage

This command sets the delay after which the control response can be terminated. The [auto-traffic-control auto-control-release](#) command must be used to enable or disable the automatic release of a control response of rate-limiting. To re-enable a port which has been shut down by automatic traffic control, you must manually re-enable the port using the [auto-traffic-control control-release](#) command.

Example

This example sets the release timer to 800 seconds for all ports.

```
Console(config)#auto-traffic-control broadcast release-timer 800
Console(config)#
```


auto-traffic-control This command enables automatic traffic control for broadcast or multicast storms. Use the **no** form to disable this feature.

Syntax

[no] auto-traffic-control {broadcast | multicast}

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ Automatic storm control can be enabled for either broadcast or multicast traffic. It cannot be enabled for both of these traffic types at the same time.
- ◆ Automatic storm control is a software level control function. Traffic storms can also be controlled at the hardware level using the [switchport packet-rate](#) command. However, only one of these control types can be applied to a port. Enabling automatic storm control on a port will disable hardware-level storm control on that port.

Example

This example enables automatic storm control for broadcast traffic on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast
Console(config-if)#
```

auto-traffic-control action This command sets the control action to limit ingress traffic or shut down the offending port. Use the **no** form to restore the default setting.

Syntax

auto-traffic-control {broadcast | multicast} action {rate-control | shutdown}

no auto-traffic-control {broadcast | multicast} action

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

rate-control - If a control response is triggered, the rate of ingress traffic is limited based on the threshold configured by the [auto-traffic-control alarm-clear-threshold](#) command.

shutdown - If a control response is triggered, the port is administratively disabled. A port disabled by automatic traffic control can only be manually re-enabled.

Default Setting

rate-control

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ When the upper threshold is exceeded and the apply timer expires, a control response will be triggered based on this command.
- ◆ When the control response is set to rate limiting by this command, the rate limits are determined by the [auto-traffic-control alarm-clear-threshold](#) command.
- ◆ If the control response is to limit the rate of ingress traffic, it can be automatically terminated once the traffic rate has fallen beneath the lower threshold and the release timer has expired.
- ◆ If a port has been shut down by a control response, it will not be re-enabled by automatic traffic control. It can only be manually re-enabled using the [auto-traffic-control control-release](#) command.

Example

This example sets the control response for broadcast traffic on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast action shutdown
Console(config-if)#
```

auto-traffic-control alarm-clear-threshold

This command sets the lower threshold for ingress traffic beneath which a control response for rate limiting will be released after the Release Timer expires, if so configured by the [auto-traffic-control auto-control-release](#) command. Use the **no** form to restore the default setting.

Syntax

auto-traffic-control {broadcast | multicast} alarm-clear-threshold *threshold*

no auto-traffic-control {broadcast | multicast} alarm-clear-threshold

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

threshold - The lower threshold for ingress traffic beneath which a cleared storm control trap is sent. (Range: 1-255 kilo-packets per second)

Default Setting

128 kilo-packets per second

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ Once the traffic rate falls beneath the lower threshold, a trap message may be sent if configured by the `snmp-server enable port-traps atc broadcast-alarm-clear` command or `snmp-server enable port-traps atc multicast-alarm-clear` command.
- ◆ If rate limiting has been configured as a control response, it will be discontinued after the traffic rate has fallen beneath the lower threshold, and the release timer has expired. Note that if a port has been shut down by a control response, it will not be re-enabled by automatic traffic control. It can only be manually re-enabled using the `auto-traffic-control control-release` command.

Example

This example sets the clear threshold for automatic storm control for broadcast traffic on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast alarm-clear-threshold 155
Console(config-if)#
```

auto-traffic-control alarm-fire-threshold

This command sets the upper threshold for ingress traffic beyond which a storm control response is triggered after the apply timer expires. Use the **no** form to restore the default setting.

Syntax

auto-traffic-control {broadcast | multicast} alarm-fire-threshold *threshold*

no auto-traffic-control {broadcast | multicast} alarm-fire-threshold

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

threshold - The upper threshold for ingress traffic beyond which a storm control response is triggered after the apply timer expires. (Range: 1-255 kilo-packets per second)

Default Setting

128 kilo-packets per second

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ Once the upper threshold is exceeded, a trap message may be sent if configured by the [snmp-server enable port-traps atc broadcast-alarm-fire](#) command or [snmp-server enable port-traps atc multicast-alarm-fire](#) command.
- ◆ After the upper threshold is exceeded, the control timer must first expire as configured by the [auto-traffic-control apply-timer](#) command before a control response is triggered if configured by the [auto-traffic-control action](#) command.

Example

This example sets the trigger threshold for automatic storm control for broadcast traffic on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast alarm-fire-threshold 255
Console(config-if)#
```

auto-traffic-control auto-control-release This command automatically releases a control response of rate-limiting after the time specified in the [auto-traffic-control release-timer](#) command has expired.

Syntax

auto-traffic-control {broadcast | multicast} auto-control-release

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ This command can be used to automatically stop a control response of rate-limiting after the specified action has been triggered and the release timer has expired.
- ◆ To release a control response which has shut down a port after the specified action has been triggered and the release timer has expired, use the [auto-traffic-control control-release](#) command.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast auto-control-release
Console(config-if)#
```

**auto-traffic-control
control-release** This command manually releases a control response.

Syntax

auto-traffic-control {broadcast | multicast} control-release

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

Command Mode

Interface Configuration (Ethernet)

Command Usage

This command can be used to manually stop a control response of rate-limiting or port shutdown any time after the specified action has been triggered.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast control-release
Console#(config-if)
```

SNMP Trap Commands

**snmp-server enable
port-traps atc
broadcast-alarm-clear** This command sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered. Use the **no** form to disable this trap.

Syntax

[no] snmp-server enable port-traps atc broadcast-alarm-clear

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc broadcast-alarm-clear
Console(config-if)#
```

Related Commands

[auto-traffic-control action \(433\)](#)

[auto-traffic-control alarm-clear-threshold \(434\)](#)

snmp-server enable port-traps atc broadcast-alarm-fire This command sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control. Use the **no** form to disable this trap.

Syntax

[no] snmp-server enable port-traps atc broadcast-alarm-fire

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc broadcast-alarm-fire
Console(config-if)#
```

Related Commands

[auto-traffic-control alarm-fire-threshold \(435\)](#)

snmp-server enable port-traps atc broadcast-control-apply This command sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control and the apply timer expires. Use the **no** form to disable this trap.

Syntax

[no] snmp-server enable port-traps atc broadcast-control-apply

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc broadcast-control-apply
Console(config-if)#
```

Related Commands

[auto-traffic-control alarm-fire-threshold \(435\)](#)

[auto-traffic-control apply-timer \(431\)](#)

snmp-server enable port-traps atc broadcast-control-release This command sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires. Use the **no** form to disable this trap.

Syntax

[no] snmp-server enable port-traps atc broadcast-control-release

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc broadcast-control-
release
Console(config-if)#
```

Related Commands

[auto-traffic-control alarm-clear-threshold \(434\)](#)

[auto-traffic-control action \(433\)](#)

[auto-traffic-control release-timer \(432\)](#)

snmp-server enable port-traps atc multicast-alarm-clear This command sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered. Use the **no** form to disable this trap.

Syntax

[no] snmp-server enable port-traps atc multicast-alarm-clear

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc multicast-alarm-clear
Console(config-if)#
```

Related Commands

[auto-traffic-control action \(433\)](#)

[auto-traffic-control alarm-clear-threshold \(434\)](#)

snmp-server enable port-traps atc multicast-alarm-fire This command sends a trap when multicast traffic exceeds the upper threshold for automatic storm control. Use the **no** form to disable this trap.

Syntax

[no] snmp-server enable port-traps atc multicast-alarm-fire

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc multicast-alarm-fire
Console(config-if)#
```

Related Commands

[auto-traffic-control alarm-fire-threshold \(435\)](#)

snmp-server enable port-traps atc multicast-control-apply This command sends a trap when multicast traffic exceeds the upper threshold for automatic storm control and the apply timer expires. Use the **no** form to disable this trap.

Syntax

[no] snmp-server enable port-traps atc multicast-control-apply

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc multicast-control-apply
Console(config-if)#
```

Related Commands

[auto-traffic-control alarm-fire-threshold \(435\)](#)

[auto-traffic-control apply-timer \(431\)](#)

snmp-server enable port-traps atc multicast-control-release This command sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires. Use the **no** form to disable this trap.

Syntax

[no] snmp-server enable port-traps atc multicast-control-release

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc multicast-control-release
Console(config-if)#
```

Related Commands

[auto-traffic-control alarm-clear-threshold \(434\)](#)

[auto-traffic-control action \(433\)](#)

[auto-traffic-control release-timer \(432\)](#)

ATC Display Commands

show auto-traffic-control This command shows global configuration settings for automatic storm control.

Command Mode

Privileged Exec

Example

```
Console#show auto-traffic-control

Storm-control: Broadcast
  Apply-timer (sec)      : 300
  release-timer (sec)    : 900

Storm-control: Multicast
  Apply-timer(sec)       : 300
  release-timer(sec)     : 900
Console#
```

show auto-traffic-control interface This command shows interface configuration settings and storm control status for the specified port.

Syntax

show auto-traffic-control interface [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

Command Mode

Privileged Exec

Example

```
Console#show auto-traffic-control interface ethernet 1/1
Eth 1/1 Information
-----
Storm Control:          Broadcast          Multicast
State:                  Disabled          Disabled
Action:                 rate-control       rate-control
Auto Release Control:   Disabled          Disabled
Alarm Fire Threshold(Kpps): 128             128
Alarm Clear Threshold(Kpps):128             128
Trap Storm Fire:        Disabled          Disabled
Trap Storm Clear:       Disabled          Disabled
Trap Traffic Apply:     Disabled          Disabled
Trap Traffic Release:   Disabled          Disabled

Console#
```

Address Table Commands

These commands are used to configure the address table for filtering specified addresses, displaying current entries, clearing the table, or setting the aging time.

Table 87: Address Table Commands

Command	Function	Mode
<code>mac-address-table aging-time</code>	Sets the aging time of the address table	GC
<code>mac-address-table static</code>	Maps a static address to a port in a VLAN	GC
<code>clear mac-address-table dynamic</code>	Removes any learned entries from the forwarding database	PE
<code>show mac-address-table</code>	Displays entries in the bridge-forwarding database	PE
<code>show mac-address-table aging-time</code>	Shows the aging time for the address table	PE
<code>show mac-address-table count</code>	Shows the number of MAC addresses used and the number of available MAC addresses	PE

mac-address-table aging-time This command sets the aging time for entries in the address table. Use the **no** form to restore the default aging time.

Syntax

mac-address-table aging-time *seconds*

no mac-address-table aging-time

seconds - Aging time. (Range: 10-1000000 seconds; 0 to disable aging)

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

The aging time is used to age out dynamically learned forwarding information.

Example

```
Console(config)#mac-address-table aging-time 100
Console(config)#
```

mac-address-table static This command maps a static address to a port in a VLAN, and optionally designates the address as permanent, or to be deleted on reset. Use the **no** form to remove an address.

Syntax

mac-address-table static *mac-address* **interface** *interface* **vlan** *vlan-id* [*action*]

no mac-address-table static *mac-address* **vlan** *vlan-id*

mac-address - MAC address.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

vlan-id - VLAN ID (Range: 1-4094)

action -

delete-on-reset - Assignment lasts until the switch is reset.

permanent - Assignment is permanent.

Default Setting

No static addresses are defined.

The default lifetime is **permanent**.

Command Mode

Global Configuration

Command Usage

The static address for a host device can be assigned to a specific port within a specific VLAN. Use this command to add static addresses to the MAC Address Table. Static addresses have the following characteristics:

- ◆ Static addresses will not be removed from the address table when a given interface link is down.
- ◆ Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.
- ◆ A static address cannot be learned on another port until the address is removed with the **no** form of this command.

Example

```
Console(config)#mac-address-table static 00-e0-29-94-34-de interface ethernet
1/1 vlan 1 delete-on-reset
Console(config)#
```

clear mac-address-table dynamic This command removes any learned entries from the forwarding database.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#clear mac-address-table dynamic
Console#
```

show mac-address-table This command shows classes of entries in the bridge-forwarding database.

Syntax

show mac-address-table [**address** *mac-address* [*mask*]] [**interface** *interface*] [**vlan** *vlan-id*] [**sort** {**address** | **vlan** | **interface**}]

mac-address - MAC address.

mask - Bits to match in the address.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

vlan-id - VLAN ID (Range: 1-4094)

sort - Sort by address, vlan or interface.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- ◆ The MAC Address Table contains the MAC addresses associated with each interface. Note that the Type field may include the following types:
 - Learn - Dynamic address entries
 - Config - Static entry
- ◆ The mask should be hexadecimal numbers (representing an equivalent bit mask) in the form xx-xx-xx-xx-xx-xx that is applied to the specified MAC address. Enter hexadecimal numbers, where an equivalent binary bit "0" means to match a bit and "1" means to ignore a bit. For example, a mask of 00-00-00-00-00-00 means an exact match, and a mask of FF-FF-FF-FF-FF-FF means "any."
- ◆ The maximum number of address entries is 16K.

Example

```

Console#show mac-address-table
Interface MAC Address      VLAN Type      Life Time
-----
CPU      00-00-0C-00-00-FD      1 CPU      Delete on Reset
Eth 1/ 1 00-E0-29-94-34-DE  1 Config   Delete on Reset
Eth 1/21 00-01-EC-F8-D8-D9  1 Learn    Delete on Timeout
Console#

```

show mac-address-table aging-time This command shows the aging time for entries in the address table.

Default Setting

None

Command Mode

Privileged Exec

Example

```

Console#show mac-address-table aging-time
Aging Status : Enabled
Aging Time: 300 sec.
Console#

```

show mac-address-table count This command shows the number of MAC addresses used and the number of available MAC addresses for the overall system or for an interface.

Syntax

show mac-address-table count interface *interface*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show mac-address-table count interface ethernet 1/1

MAC Entries for Port ID   :1
Dynamic Address Count     :2
Total MAC Addresses       :2
Total MAC Address Space Available: 32768
Console#
```


Spanning Tree Commands

This section includes commands that configure the Spanning Tree Algorithm (STA) globally for the switch, and commands that configure STA for the selected interface.

Table 88: Spanning Tree Commands

Command	Function	Mode
<code>spanning-tree</code>	Enables the spanning tree protocol	GC
<code>spanning-tree forward-time</code>	Configures the spanning tree bridge forward time	GC
<code>spanning-tree hello-time</code>	Configures the spanning tree bridge hello time	GC
<code>spanning-tree max-age</code>	Configures the spanning tree bridge maximum age	GC
<code>spanning-tree mode</code>	Configures STP, RSTP or MSTP mode	GC
<code>spanning-tree pathcost method</code>	Configures the path cost method for RSTP/MSTP	GC
<code>spanning-tree priority</code>	Configures the spanning tree bridge priority	GC
<code>spanning-tree mst configuration</code>	Changes to MSTP configuration mode	GC
<code>spanning-tree system-bpdu-flooding</code>	Floods BPDUs to all other ports or just to all other ports in the same VLAN when global spanning tree is disabled	GC
<code>spanning-tree transmission-limit</code>	Configures the transmission limit for RSTP/MSTP	GC
<code>max-hops</code>	Configures the maximum number of hops allowed in the region before a BPDU is discarded	MST
<code>mst priority</code>	Configures the priority of a spanning tree instance	MST
<code>mst vlan</code>	Adds VLANs to a spanning tree instance	MST
<code>name</code>	Configures the name for the multiple spanning tree	MST
<code>revision</code>	Configures the revision number for the multiple spanning tree	MST
<code>spanning-tree bpdu-filter</code>	Filters BPDUs for edge ports	IC
<code>spanning-tree bpdu-guard</code>	Shuts down an edge port if it receives a BPDU	IC
<code>spanning-tree cost</code>	Configures the spanning tree path cost of an interface	IC
<code>spanning-tree edge-port</code>	Enables fast forwarding for edge ports	IC
<code>spanning-tree link-type</code>	Configures the link type for RSTP/MSTP	IC
<code>spanning-tree loopback-detection</code>	Enables BPDU loopback detection for a port	IC
<code>spanning-tree loopback-detection action</code>	Configures the response for loopback detection to block user traffic or shut down the interface	IC

Table 88: Spanning Tree Commands (Continued)

Command	Function	Mode
<code>spanning-tree loopback-detection release-mode</code>	Configures loopback release mode for a port	IC
<code>spanning-tree loopback-detection trap</code>	Enables BPDU loopback SNMP trap notification for a port	IC
<code>spanning-tree mst cost</code>	Configures the path cost of an instance in the MST	IC
<code>spanning-tree mst port-priority</code>	Configures the priority of an instance in the MST	IC
<code>spanning-tree port-bpdu-flooding</code>	Floods BPDUs to other ports when global spanning tree is disabled	IC
<code>spanning-tree port-priority</code>	Configures the spanning tree priority of an interface	IC
<code>spanning-tree root-guard</code>	Prevents a designated port from passing superior BPDUs	IC
<code>spanning-tree spanning-disabled</code>	Disables spanning tree for an interface	IC
<code>spanning-tree loopback-detection release</code>	Manually releases a port placed in discarding state by loopback-detection	PE
<code>spanning-tree protocol-migration</code>	Re-checks the appropriate BPDU format	PE
<code>show spanning-tree</code>	Shows spanning tree configuration for the common spanning tree (i.e., overall bridge), a selected interface, or an instance within the multiple spanning tree	PE
<code>show spanning-tree mst configuration</code>	Shows the multiple spanning tree configuration	PE

spanning-tree This command enables the Spanning Tree Algorithm globally for the switch. Use the **no** form to disable it.

Syntax

[no] spanning-tree

Default Setting

Spanning tree is enabled.

Command Mode

Global Configuration

Command Usage

The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

Example

This example shows how to enable the Spanning Tree Algorithm for the switch:

```
Console(config)#spanning-tree
Console(config)#
```

spanning-tree forward-time This command configures the spanning tree bridge forward time globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree forward-time *seconds*

no spanning-tree forward-time

seconds - Time in seconds. (Range: 4 - 30 seconds)

The minimum value is the higher of 4 or $[(\text{max-age} / 2) + 1]$.

Default Setting

15 seconds

Command Mode

Global Configuration

Command Usage

This command sets the maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to the discarding state; otherwise, temporary data loops might result.

Example

```
Console(config)#spanning-tree forward-time 20
Console(config)#
```

spanning-tree hello-time This command configures the spanning tree bridge hello time globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree hello-time *time*

no spanning-tree hello-time

time - Time in seconds. (Range: 1-10 seconds).

The maximum value is the lower of 10 or $[(\text{max-age} / 2) - 1]$.

Default Setting

2 seconds

Command Mode

Global Configuration

Command Usage

This command sets the time interval (in seconds) at which the root device transmits a configuration message.

Example

```
Console(config)#spanning-tree hello-time 5
Console(config)#
```

Related Commands

[spanning-tree forward-time \(451\)](#)

[spanning-tree max-age \(452\)](#)

spanning-tree max-age This command configures the spanning tree bridge maximum age globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree max-age *seconds*

no spanning-tree max-age

seconds - Time in seconds. (Range: 6-40 seconds)

The minimum value is the higher of 6 or $[2 \times (\text{hello-time} + 1)]$.

The maximum value is the lower of 40 or $[2 \times (\text{forward-time} - 1)]$.

Default Setting

20 seconds

Command Mode

Global Configuration

Command Usage

This command sets the maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconverge. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.

Example

```
Console(config)#spanning-tree max-age 40
Console(config)#
```

Related Commands

[spanning-tree forward-time \(451\)](#)

[spanning-tree hello-time \(452\)](#)

spanning-tree mode This command selects the spanning tree mode for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree mode {stp | rstp | mstp}

no spanning-tree mode

stp - Spanning Tree Protocol (IEEE 802.1D)

rstp - Rapid Spanning Tree Protocol (IEEE 802.1w)

mstp - Multiple Spanning Tree (IEEE 802.1s)

Default Setting

rstp

Command Mode

Global Configuration

Command Usage

- ◆ **Spanning Tree Protocol**
This option uses RSTP set to STP forced compatibility mode. It uses RSTP for the internal state machine, but sends only 802.1D BPDUs. This creates one spanning tree instance for the entire network. If multiple VLANs are implemented on a network, the path between specific VLAN members may be inadvertently disabled to prevent network loops, thus isolating group members. When operating multiple VLANs, we recommend selecting the MSTP option.
- ◆ **Rapid Spanning Tree Protocol**
RSTP supports connections to either STP or RSTP nodes by monitoring the

incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:

- STP Mode – If the switch receives an 802.1D BPDU after a port's migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.
- RSTP Mode – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.

◆ Multiple Spanning Tree Protocol

- To allow multiple spanning trees to operate over the network, you must configure a related set of bridges with the same MSTP configuration, allowing them to participate in a specific set of spanning tree instances.
- A spanning tree instance can exist only on bridges that have compatible VLAN instance assignments.
- Be careful when switching between spanning tree modes. Changing modes stops all spanning-tree instances for the previous mode and restarts the system in the new mode, temporarily disrupting user traffic.

Example

The following example configures the switch to use Rapid Spanning Tree:

```
Console(config)#spanning-tree mode rstp
Console(config)#
```

spanning-tree pathcost method

This command configures the path cost method used for Rapid Spanning Tree and Multiple Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree pathcost method {long | short}

no spanning-tree pathcost method

long - Specifies 32-bit based values that range from 1-200,000,000.
This method is based on the IEEE 802.1w Rapid Spanning Tree Protocol.

short - Specifies 16-bit based values that range from 1-65535.
This method is based on the IEEE 802.1 Spanning Tree Protocol.

Default Setting

Long method

Command Mode

Global Configuration

Command Usage

- ◆ The path cost method is used to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Note that path cost ([page 463](#)) takes precedence over port priority ([page 471](#)).
- ◆ The path cost methods apply to all spanning tree modes (STP, RSTP and MSTP). Specifically, the long method can be applied to STP since this mode is supported by a backward compatible mode of RSTP.

Example

```
Console(config)#spanning-tree pathcost method long
Console(config)#
```

spanning-tree priority This command configures the spanning tree priority globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree priority *priority*

no spanning-tree priority

priority - Priority of the bridge. (Range – 0-61440, in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

Default Setting

32768

Command Mode

Global Configuration

Command Usage

Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority (i.e., lower numeric value) becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.

Example

```
Console(config)#spanning-tree priority 40000
Console(config)#
```

spanning-tree mst configuration This command changes to Multiple Spanning Tree (MST) configuration mode.

Syntax

spanning-tree mst configuration

Default Setting

No VLANs are mapped to any MST instance.
The region name is set the switch's MAC address.

Command Mode

Global Configuration

Example

```
Console(config)#spanning-tree mst configuration
Console(config-mstp)#
```

Related Commands

[mst vlan \(459\)](#)
[mst priority \(458\)](#)
[name \(460\)](#)
[revision \(460\)](#)
[max-hops \(457\)](#)

spanning-tree system-bpdu-flooding This command configures the system to flood BPDUs to all other ports on the switch or just to all other ports in the same VLAN when spanning tree is disabled globally on the switch or disabled on a specific port. Use the **no** form to restore the default.

Syntax

spanning-tree system-bpdu-flooding {to-all | to-vlan}

no spanning-tree system-bpdu-flooding

to-all - Floods BPDUs to all other ports on the switch.

to-vlan - Floods BPDUs to all other ports within the receiving port's native VLAN (i.e., as determined by port's PVID).

Default Setting

Floods to all other ports in the same VLAN.

Command Mode

Global Configuration

Command Usage

The **spanning-tree system-bpdu-flooding** command has no effect if BPDU flooding is disabled on a port (see the [spanning-tree port-bpdu-flooding](#) command).

Example

```
Console(config)#spanning-tree system-bpdu-flooding
Console(config)#
```

spanning-tree transmission-limit

This command configures the minimum interval between the transmission of consecutive RSTP/MSTP BPDUs. Use the **no** form to restore the default.

Syntax

spanning-tree transmission-limit *count*

no spanning-tree transmission-limit

count - The transmission limit in seconds. (Range: 1-10)

Default Setting

3

Command Mode

Global Configuration

Command Usage

This command limits the maximum transmission rate for BPDUs.

Example

```
Console(config)#spanning-tree transmission-limit 4
Console(config)#
```

max-hops

This command configures the maximum number of hops in the region before a BPDU is discarded. Use the **no** form to restore the default.

Syntax

max-hops *hop-number*

hop-number - Maximum hop number for multiple spanning tree.
(Range: 1-40)

Default Setting

20

Command Mode

MST Configuration

Command Usage

An MSTI region is treated as a single node by the STP and RSTP protocols. Therefore, the message age for BPDUs inside an MSTI region is never changed. However, each spanning tree instance within a region, and the internal spanning tree (IST) that connects these instances use a hop count to specify the maximum number of bridges that will propagate a BPDU. Each bridge decrements the hop count by one before passing on the BPDU. When the hop count reaches zero, the message is dropped.

Example

```
Console(config-mstp) #max-hops 30
Console(config-mstp) #
```

mst priority This command configures the priority of a spanning tree instance. Use the **no** form to restore the default.

Syntax

mst *instance-id* **priority** *priority*

no mst *instance-id* **priority**

instance-id - Instance identifier of the spanning tree.
(Range: 0-4094)

priority - Priority of the a spanning tree instance.
(Range: 0-61440 in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

Default Setting

32768

Command Mode

MST Configuration

Command Usage

- ◆ MST priority is used in selecting the root bridge and alternate bridge of the specified instance. The device with the highest priority (i.e., lowest numerical value) becomes the MSTI root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.
- ◆ You can set this switch to act as the MSTI root device by specifying a priority of 0, or as the MSTI alternate device by specifying a priority of 16384.

Example

```
Console(config-mstp)#mst 1 priority 4096
Console(config-mstp)#
```

mst vlan This command adds VLANs to a spanning tree instance. Use the **no** form to remove the specified VLANs. Using the **no** form without any VLAN parameters to remove all VLANs.

Syntax

[no] mst instance-id vlan vlan-range

instance-id - Instance identifier of the spanning tree. (Range: 0-4094)

vlan-range - Range of VLANs. (Range: 1-4094)

Default Setting

none

Command Mode

MST Configuration

Command Usage

- ◆ Use this command to group VLANs into spanning tree instances. MSTP generates a unique spanning tree for each instance. This provides multiple pathways across the network, thereby balancing the traffic load, preventing wide-scale disruption when a bridge node in a single instance fails, and allowing for faster convergence of a new topology for the failed instance.
- ◆ By default all VLANs are assigned to the Internal Spanning Tree (MSTI 0) that connects all bridges and LANs within the MST region. This switch supports up to 33 instances. You should try to group VLANs which cover the same general area of your network. However, remember that you must configure all bridges within the same MSTI Region ([page 460](#)) with the same set of instances, and the same instance (on each bridge) with the same set of VLANs. Also, note that RSTP treats each MSTI region as a single node, connecting all regions to the Common Spanning Tree.

Example

```
Console(config-mstp)#mst 1 vlan 2-5
Console(config-mstp)#
```

name This command configures the name for the multiple spanning tree region in which this switch is located. Use the **no** form to clear the name.

Syntax

name *name*

name - Name of the spanning tree.

Default Setting

Switch's MAC address

Command Mode

MST Configuration

Command Usage

The MST region name and revision number ([page 460](#)) are used to designate a unique MST region. A bridge (i.e., spanning-tree compliant device such as this switch) can only belong to one MST region. And all bridges in the same region must be configured with the same MST instances.

Example

```
Console(config-mstp)#name R&D
Console(config-mstp)#
```

Related Commands

[revision \(460\)](#)

revision This command configures the revision number for this multiple spanning tree configuration of this switch. Use the **no** form to restore the default.

Syntax

revision *number*

number - Revision number of the spanning tree. (Range: 0-65535)

Default Setting

0

Command Mode

MST Configuration

Command Usage

The MST region name ([page 460](#)) and revision number are used to designate a unique MST region. A bridge (i.e., spanning-tree compliant device such as this switch) can only belong to one MST region. And all bridges in the same region must be configured with the same MST instances.

Example

```
Console(config-mstp)#revision 1
Console(config-mstp)#
```

Related Commands

[name \(460\)](#)

spanning-tree bpd-filter This command filters all BPDUs received on an edge port. Use the **no** form to disable this feature.

Syntax

[no] spanning-tree bpd-filter

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ This command filters all Bridge Protocol Data Units (BPDUs) received on an interface to save CPU processing time. This function is designed to work in conjunction with edge ports which should only connect end stations to the switch, and therefore do not need to process BPDUs. However, note that if a trunking port connected to another switch or bridging device is mistakenly configured as an edge port, and BPDU filtering is enabled on this port, this might cause a loop in the spanning tree.
- ◆ Before enabling BPDU Filter, the interface must first be configured as an edge port with the [spanning-tree edge-port](#) command.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#spanning-tree bpd-filter
Console(config-if)#
```

Related Commands

[spanning-tree edge-port \(464\)](#)

spanning-tree bpduguard This command shuts down an edge port (i.e., an interface set for fast forwarding) if it receives a BPDU. Use the **no** form without any keywords to disable this feature, or with a keyword to restore the default settings.

Syntax

spanning-tree bpduguard [**auto-recovery** [**interval** *interval*]]

no spanning-tree bpduguard [**auto-recovery** [**interval**]]

auto-recovery - Automatically re-enables an interface after the specified interval.

interval - The time to wait before re-enabling an interface. (Range: 30-86400 seconds)

Default Setting

BPDU Guard: Disabled

Auto-Recovery: Disabled

Auto-Recovery Interval: 300 seconds

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ An edge port should only be connected to end nodes which do not generate BPDUs. If a BPDU is received on an edge port, this indicates an invalid network configuration, or that the switch may be under attack by a hacker. If an interface is shut down by BPDU Guard, it must be manually re-enabled using the [no spanning-tree spanning-disabled](#) command if the auto-recovery interval is not specified.
- ◆ Before enabling BPDU Guard, the interface must be configured as an edge port with the [spanning-tree edge-port](#) command. Also note that if the edge port attribute is disabled on an interface, BPDU Guard will also be disabled on that interface.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#spanning-tree bpduguard
Console(config-if)#
```

Related Commands

[spanning-tree edge-port \(464\)](#)

[spanning-tree spanning-disabled \(472\)](#)

spanning-tree cost This command configures the spanning tree path cost for the specified interface. Use the **no** form to restore the default auto-configuration mode.

Syntax

spanning-tree cost *cost*

no spanning-tree cost

cost - The path cost for the port. (Range: 0 for auto-configuration, 1-65535 for short path cost method⁹, 1-200,000,000 for long path cost method)

Table 89: Recommended STA Path Cost Range

Port Type	Short Path Cost (IEEE 802.1D-1998)	Long Path Cost (802.1D-2004)
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000
10G Ethernet	1-5	200-20,000
40G Ethernet	1-65535 ¹	20-2,000 ¹

¹ Undefined in standard.

Default Setting

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost "0" is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

Table 90: Default STA Path Costs

Port Type	Short Path Cost (IEEE 802.1D-1998)	Long Path Cost (802.1D-2004)
Ethernet	65,535	1,000,000
Fast Ethernet	65,535	100,000
Gigabit Ethernet	10,000	10,000
10G Ethernet	1,000	1,000
40G Ethernet	65535 ¹	2,000,000 ²

¹ Undefined in standard, but recommended setting is 250.

² Code does not support 40G path cost, and therefore defaults to 10M half duplex cost.

Command Mode

Interface Configuration (Ethernet, Port Channel)

- Use the [spanning-tree pathcost method](#) command on [page 454](#) to set the path cost method.

Command Usage

- ◆ This command is used by the Spanning Tree Algorithm to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media.
- ◆ Path cost takes precedence over port priority.
- ◆ When the path cost method ([page 454](#)) is set to short, the maximum value for path cost is 65,535.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree cost 50
Console(config-if)#
```

spanning-tree edge-port This command specifies an interface as an edge port. Use the **no** form to restore the default.

Syntax

spanning-tree edge-port [auto]

no spanning-tree edge-port

auto - Automatically determines if an interface is an edge port.

Default Setting

Auto

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related time out problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.

Example

```

Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#

```

spanning-tree link-type This command configures the link type for Rapid Spanning Tree and Multiple Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree link-type {auto | point-to-point | shared}

no spanning-tree link-type

auto - Automatically derived from the duplex mode setting.

point-to-point - Point-to-point link.

shared - Shared medium.

Default Setting

auto

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ Specify a point-to-point link if the interface can only be connected to exactly one other bridge, or a shared link if it can be connected to two or more bridges.
- ◆ When automatic detection is selected, the switch derives the link type from the duplex mode. A full-duplex interface is considered a point-to-point link, while a half-duplex interface is assumed to be on a shared link.
- ◆ RSTP only works on point-to-point links between two bridges. If you designate a port as a shared link, RSTP is forbidden. Since MSTP is an extension of RSTP, this same restriction applies.

Example

```

Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree link-type point-to-point

```

spanning-tree loopback-detection This command enables the detection and response to Spanning Tree loopback BPDUs on the port. Use the **no** form to disable this feature.

Syntax

[no] spanning-tree loopback-detection

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ If Port Loopback Detection is not enabled and a port receives its own BPDU, then the port will drop the loopback BPDU according to IEEE Standard 802.1W-2001 9.3.4 (Note 1).
- ◆ Port Loopback Detection will not be active if Spanning Tree is disabled on the switch.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection
```

spanning-tree loopback-detection action This command configures the response for loopback detection to block user traffic or shut down the interface. Use the **no** form to restore the default.

Syntax

spanning-tree loopback-detection action
{block | shutdown duration}

no spanning-tree loopback-detection action

block - Blocks user traffic.

shutdown - Shuts down the interface.

duration - The duration to shut down the interface.
(Range: 60-86400 seconds)

Default Setting

block

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ If an interface is shut down by this command, and the release mode is set to "auto" with the `spanning-tree loopback-detection release-mode` command, the selected interface will be automatically enabled when the shutdown interval has expired.
- ◆ If an interface is shut down by this command, and the release mode is set to "manual," the interface can be re-enabled using the `spanning-tree loopback-detection release` command.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection action shutdown 600
```

spanning-tree loopback-detection release-mode

This command configures the release mode for a port that was placed in the discarding state because a loopback BPDU was received. Use the **no** form to restore the default.

Syntax

spanning-tree loopback-detection release-mode
{auto | manual}

no spanning-tree loopback-detection release-mode

auto - Allows a port to automatically be released from the discarding state when the loopback state ends.

manual - The port can only be released from the discarding state manually.

Default Setting

auto

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ If the port is configured for automatic loopback release, then the port will only be returned to the forwarding state if one of the following conditions is satisfied:
 - The port receives any other BPDU except for its own, or;
 - The port's link status changes to link down and then link up again, or;
 - The port ceases to receive its own BPDUs in a forward delay interval.
- ◆ If Port Loopback Detection is not enabled and a port receives its own BPDU, then the port will drop the loopback BPDU according to IEEE Standard 802.1W-2001 9.3.4 (Note 1).

- ◆ Port Loopback Detection will not be active if Spanning Tree is disabled on the switch.
- ◆ When configured for manual release mode, then a link down / up event will not release the port from the discarding state. It can only be released using the `spanning-tree loopback-detection release` command.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection release-mode manual
Console(config-if)#
```

spanning-tree loopback-detection trap

This command enables SNMP trap notification for Spanning Tree loopback BPDU detections. Use the **no** form to restore the default.

Syntax

[no] spanning-tree loopback-detection trap

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection trap
```

spanning-tree mst cost

This command configures the path cost on a spanning instance in the Multiple Spanning Tree. Use the **no** form to restore the default auto-configuration mode.

Syntax

spanning-tree mst *instance-id* cost *cost*

no spanning-tree mst *instance-id* cost

instance-id - Instance identifier of the spanning tree. (Range: 0-4094)

cost - Path cost for an interface. (Range: 0 for auto-configuration, 1-65535 for short path cost method¹⁰, 1-200,000,000 for long path cost method)

The recommended path cost range is listed in [Table 89 on page 463](#).

Default Setting

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path

cost "0" is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535. The default path costs are listed in [Table 90 on page 463](#).

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ Each spanning-tree instance is associated with a unique set of VLAN IDs.
- ◆ This command is used by the multiple spanning-tree algorithm to determine the best path between devices. Therefore, lower values should be assigned to interfaces attached to faster media, and higher values assigned to interfaces with slower media.
- ◆ Use the **no spanning-tree mst cost** command to specify auto-configuration mode.
- ◆ Path cost takes precedence over interface priority.

Example

```
Console(config)#interface Ethernet 1/5
Console(config-if)#spanning-tree mst 1 cost 50
Console(config-if)#
```

Related Commands

[spanning-tree mst port-priority \(469\)](#)

spanning-tree mst port-priority This command configures the interface priority on a spanning instance in the Multiple Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree mst *instance-id* **port-priority** *priority*

no spanning-tree mst *instance-id* **port-priority**

instance-id - Instance identifier of the spanning tree. (Range: 0-4094)

priority - Priority for an interface. (Range: 0-240 in steps of 16)

Default Setting

128

Command Mode

Interface Configuration (Ethernet, Port Channel)

10. Use the [spanning-tree pathcost method](#) command to set the path cost method.

Command Usage

- ◆ This command defines the priority for the use of an interface in the multiple spanning-tree. If the path cost for all interfaces on a switch are the same, the interface with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.
- ◆ Where more than one interface is assigned the highest priority, the interface with lowest numeric identifier will be enabled.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree mst 1 port-priority 0
Console(config-if)#
```

Related Commands

[spanning-tree mst cost \(468\)](#)

spanning-tree port-bpdu-flooding

This command floods BPDUs to other ports when spanning tree is disabled globally or disabled on a specific port. Use the **no** form to restore the default setting.

Syntax

[no] spanning-tree port-bpdu-flooding

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ When enabled, BPDUs are flooded to all other ports on the switch or to all other ports within the receiving port's native VLAN as specified by the [spanning-tree system-bpdu-flooding](#) command.
- ◆ The [spanning-tree system-bpdu-flooding](#) command has no effect if BPDU flooding is disabled on a port by the **spanning-tree port-bpdu-flooding** command.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-bpdu-flooding
Console(config-if)#
```

spanning-tree port-priority This command configures the priority for the specified interface. Use the **no** form to restore the default.

Syntax

spanning-tree port-priority *priority*

no spanning-tree port-priority

priority - The priority for a port. (Range: 0-240, in steps of 16)

Default Setting

128

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ This command defines the priority for the use of a port in the Spanning Tree Algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.
- ◆ Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-priority 0
```

Related Commands

[spanning-tree cost \(463\)](#)

spanning-tree root-guard This command prevents a designated port from taking superior BPDUs into account and allowing a new STP root port to be elected. Use the **no** form to disable this feature.

Syntax

[no] spanning-tree root-guard

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ A port connecting a LAN through the bridge to the root bridge is known as a designated port. A bridge with a designated port and a lower bridge identifier (or same identifier and lower MAC address) can take over as the root bridge at any time.
- ◆ When Root Guard is enabled, and the switch receives a superior BPDU on this port, it is set to the Discarding state until it stops receiving superior BPDUs for a fixed recovery period. While in the discarding state, no traffic is forwarded across the port.
- ◆ Root Guard can be used to ensure that the root bridge is not formed at a suboptimal location. Root Guard should be enabled on any designated port connected to low-speed bridges which could potentially overload a slower link by taking over as the root port and forming a new spanning tree topology. It could also be used to form a border around part of the network where the root bridge is allowed.
- ◆ When spanning tree is initialized globally on the switch or on an interface, the switch will wait for 20 seconds to ensure that the spanning tree has converged before enabling Root Guard.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#spanning-tree root-guard
Console(config-if)#
```

spanning-tree spanning-disabled This command disables the spanning tree algorithm for the specified interface. Use the **no** form to re-enable the spanning tree algorithm for the specified interface.

Syntax

[no] spanning-tree spanning-disabled

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

This example disables the spanning tree algorithm for port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree spanning-disabled
Console(config-if)#
```


spanning-tree loopback-detection release This command manually releases a port placed in discarding state by loopback-detection.

Syntax

spanning-tree loopback-detection release *interface*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Command Mode

Privileged Exec

Command Usage

Use this command to release an interface from discarding state if loopback detection release mode is set to “manual” by the [spanning-tree loopback-detection release-mode](#) command and BPDU loopback occurs.

Example

```
Console#spanning-tree loopback-detection release ethernet 1/1
Console#
```

spanning-tree protocol-migration This command re-checks the appropriate BPDU format to send on the selected interface.

Syntax

spanning-tree protocol-migration *interface*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Command Mode

Privileged Exec

Command Usage

If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the **spanning-tree protocol-**

migration command at any time to manually re-check the appropriate BPDU format to send on the selected interfaces (i.e., RSTP or STP-compatible).

Example

```
Console#spanning-tree protocol-migration eth 1/5
Console#
```

show spanning-tree This command shows the configuration for the common spanning tree (CST), for all instances within the multiple spanning tree (MST), or for a specific instance within the multiple spanning tree (MST).

Syntax

show spanning-tree [*interface* | **mst** *instance-id*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

instance-id - Instance identifier of the multiple spanning tree.
(Range: 0-4094, no leading zeroes)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- ◆ Use the **show spanning-tree** command with no parameters to display the spanning tree configuration for the switch for the Common Spanning Tree (CST) and for every interface in the tree.
- ◆ Use the **show spanning-tree interface** command to display the spanning tree configuration for an interface within the Common Spanning Tree (CST).
- ◆ Use the **show spanning-tree mst** command to display the spanning tree configuration for all instances within the Multiple Spanning Tree (MST), including global settings and settings for active interfaces.
- ◆ Use the **show spanning-tree mst instance-id** command to display the spanning tree configuration for an instance within the Multiple Spanning Tree (MST), including global settings and settings for all interfaces.

Example

```

Console#show spanning-tree
Spanning Tree Information
-----
Spanning Tree Mode           : MSTP
Spanning Tree Enabled/Disabled : Enabled
Instance                     : 0
VLANs Configured             : 1-4094
Priority                      : 32768
Bridge Hello Time (sec.)     : 2
Bridge Max. Age (sec.)       : 20
Bridge Forward Delay (sec.)  : 15
Root Hello Time (sec.)       : 2
Root Max. Age (sec.)         : 20
Root Forward Delay (sec.)    : 15
Max. Hops                     : 20
Remaining Hops                : 20
Designated Root               : 32768.0.0001ECF8D8C6
Current Root Port             : 21
Current Root Cost              : 100000
Number of Topology Changes    : 5
Last Topology Change Time (sec.): 11409
Transmission Limit            : 3
Path Cost Method              : Long
Flooding Behavior              : To VLAN
-----

Eth 1/ 1 information
-----
Admin Status                  : Enabled
Role                          : Disabled
State                         : Discarding
External Admin Path Cost      : 0
Internal Admin Path Cost      : 0
External Oper Path Cost       : 100000
Internal Oper Path Cost       : 100000
Priority                      : 128
Designated Cost               : 100000
Designated Port               : 128.1
Designated Root               : 32768.0.0001ECF8D8C6
Designated Bridge             : 32768.0.123412341234
Forward Transitions           : 4
Admin Edge Port               : Disabled
Oper Edge Port                : Disabled
Admin Link Type               : Auto
Oper Link Type                : Point-to-point
Flooding Behavior              : Enabled
Spanning-Tree Status         : Enabled
Loopback Detection Status     : Enabled
Loopback Detection Release Mode : Auto
Loopback Detection Trap       : Disabled
Loopback Detection Action     : Block
Root Guard Status             : Disabled
BPDU Guard Status             : Disabled
BPDU Guard Auto Recovery      : Disabled
BPDU Guard Auto Recovery Interval : 300
BPDU Filter Status            : Disabled
.
.
.

```

show spanning-tree mst configuration This command shows the configuration of the multiple spanning tree.

Command Mode
Privileged Exec

Example

```
Console#show spanning-tree mst configuration
Mstp Configuration Information
-----
Configuration Name : R&D
Revision Level      :0

Instance VLANs
-----
      0      1-4094
Console#
```

VLAN Commands

A VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment. This section describes commands used to create VLAN groups, add port members, specify how VLAN tagging is used, and enable automatic VLAN registration for the selected interface.

Table 91: VLAN Commands

Command Group	Function
GVRP and Bridge Extension Commands	Configures GVRP settings that permit automatic VLAN learning; shows the configuration for bridge extension MIB
Editing VLAN Groups	Sets up VLAN groups, including name, VID and state
Configuring VLAN Interfaces	Configures VLAN interface parameters, including ingress and egress tagging mode, ingress filtering, PVID, and GVRP
Displaying VLAN Information	Displays VLAN groups, status, port members, and MAC addresses
Configuring IEEE 802.1Q Tunneling	Configures 802.1Q Tunneling (QinQ Tunneling)
Configuring L2CP Tunneling*	Configures Layer 2 Control Protocol (L2CP) tunneling, either by discarding, processing, or transparently passing control packets across a QinQ tunnel
Configuring VLAN Translation*	Maps VLAN ID between customer and service provider for networks that do not support IEEE 802.1Q tunneling
Configuring Private VLANs	Configures private VLANs, including uplink and downlink ports
Configuring Protocol-based VLANs	Configures protocol-based VLANs based on frame type and protocol
Configuring IP Subnet VLANs	Configures IP Subnet-based VLANs
Configuring MAC Based VLANs	Configures MAC-based VLANs
Configuring Voice VLANs	Configures VoIP traffic detection and enables a Voice VLAN

* These functions are not compatible.

GVRP and Bridge Extension Commands

GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network. This section describes how to enable GVRP for individual interfaces and globally for the switch, as well as how to display default configuration settings for the Bridge Extension MIB.

Table 92: GVRP and Bridge Extension Commands

Command	Function	Mode
<code>bridge-ext gvrp</code>	Enables GVRP globally for the switch	GC
<code>garp timer</code>	Sets the GARP timer for the selected function	IC
<code>switchport forbidden vlan</code>	Configures forbidden VLANs for an interface	IC
<code>switchport gvrp</code>	Enables GVRP for an interface	IC
<code>show bridge-ext</code>	Shows the global bridge extension configuration	PE
<code>show garp timer</code>	Shows the GARP timer for the selected function	NE, PE
<code>show gvrp configuration</code>	Displays GVRP configuration for the selected interface	NE, PE

bridge-ext gvrp This command enables GVRP globally for the switch. Use the **no** form to disable it.

Syntax

[no] bridge-ext gvrp

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

GVRP defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. This function should be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch.

Example

```
Console(config)#bridge-ext gvrp
Console(config)#
```

garp timer This command sets the values for the join, leave and leaveall timers. Use the **no** form to restore the timers' default values.

Syntax

garp timer {join | leave | leaveall} timer-value

no garp timer {join | leave | leaveall}

{join | leave | leaveall} - Timer to set.

timer-value - Value of timer.

Ranges:

join: 20-1000 centiseconds

leave: 60-3000 centiseconds

leaveall: 500-18000 centiseconds

Default Setting

join: 20 centiseconds

leave: 60 centiseconds

leaveall: 1000 centiseconds

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ Group Address Registration Protocol is used by GVRP and GMRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless you are experiencing difficulties with GMRP or GVRP registration/deregistration.
- ◆ Timer values are applied to GVRP for all the ports on all VLANs.
- ◆ Timer values must meet the following restrictions:
 - leave \geq (3 x join)
 - leaveall > leave



Note: Set GVRP timers on all Layer 2 devices connected in the same network to the same values. Otherwise, GVRP may not operate successfully.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#garp timer join 100
Console(config-if)#
```

Related Commands

[show garp timer \(482\)](#)

switchport forbidden vlan This command configures forbidden VLANs. Use the **no** form to remove the list of forbidden VLANs.

Syntax

switchport forbidden vlan {**add** *vlan-list* | **remove** *vlan-list*}

no switchport forbidden vlan

add *vlan-list* - List of VLAN identifiers to add.

remove *vlan-list* - List of VLAN identifiers to remove.

vlan-list - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. (Range: 1-4094).

Default Setting

No VLANs are included in the forbidden list.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ This command prevents a VLAN from being automatically added to the specified interface via GVRP.
- ◆ If a VLAN has been added to the set of allowed VLANs for an interface, then you cannot add it to the set of forbidden VLANs for that same interface.

Example

The following example shows how to prevent port 1 from being added to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport forbidden vlan add 3
Console(config-if)#
```

switchport gvrp This command enables GVRP for a port. Use the **no** form to disable it.

Syntax

[no] switchport gvrp

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport gvrp
Console(config-if)#
```

show bridge-ext This command shows the configuration for bridge extension commands.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Example

```
Console#show bridge-ext
Maximum Supported VLAN Numbers      : 4094
Maximum Supported VLAN ID           : 4094
Extended Multicast Filtering Services : No
Static Entry Individual Port         : Yes
VLAN Learning                       : IVL
Configurable PVID Tagging            : Yes
Local VLAN Capable                   : No
Traffic Classes                      : Enabled
Global GVRP Status                   : Disabled
GMRP                                 : Disabled
Console#
```

Table 93: show bridge-ext - display description

Field	Description
Maximum Supported VLAN Numbers	The maximum number of VLANs supported on this switch.
Maximum Supported VLAN ID	The maximum configurable VLAN identifier supported on this switch.
Extended Multicast Filtering Services	This switch does not support the filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol).
Static Entry Individual Port	This switch allows static filtering for unicast and multicast addresses. (Refer to the mac-address-table static command.)
VLAN Learning	This switch uses Independent VLAN Learning (IVL), where each port maintains its own filtering database.
Configurable PVID Tagging	This switch allows you to override the default Port VLAN ID (PVID used in frame tags) and egress status (VLAN-Tagged or Untagged) on each port. (Refer to the switchport allowed vlan command.)
Local VLAN Capable	This switch does not support multiple local bridges outside of the scope of 802.1Q defined VLANs.

Table 93: show bridge-ext - display description (Continued)

Field	Description
Traffic Classes	This switch provides mapping of user priorities to multiple traffic classes. (Refer to “Class of Service Commands” on page 527.)
Global GVRP Status	GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network. This field shows if GVRP is globally enabled or disabled. (Refer to the bridge-ext gvrp command.)

show garp timer This command shows the GARP timers for the selected interface.

Syntax

show garp timer [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Default Setting

Shows all GARP timers.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show garp timer ethernet 1/1
Eth 1/ 1 GARP Timer Status:
Join Timer       : 20 centiseconds
Leave Timer       : 60 centiseconds
Leave All Timer   : 1000 centiseconds
Console#
```

Related Commands

[garp timer \(479\)](#)

show gvrp configuration This command shows if GVRP is enabled.

Syntax

show gvrp configuration [*interface*]
interface
ethernet *unit/port*
unit - Unit identifier. (Range: 1)
port - Port number. (Range: 1-52)
port-channel *channel-id* (Range: 1-8)

Default Setting

Shows both global and interface-specific configuration.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show gvrp configuration ethernet 1/7
Eth 1/ 7:
  GVRP Configuration : Disabled
Console#
```

Editing VLAN Groups

Table 94: Commands for Editing VLAN Groups

Command	Function	Mode
vlan database	Enters VLAN database mode to add, change, and delete VLANs	GC
vlan	Configures a VLAN, including VID, name and state	VC

vlan database This command enters VLAN database mode. All commands in this mode will take effect immediately.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ Use the VLAN database command mode to add, change, and delete VLANs. After finishing configuration changes, you can display the VLAN settings by entering the [show vlan](#) command.
- ◆ Use the [interface vlan](#) command mode to define the port membership mode and add or remove ports from a VLAN. The results of these commands are written to the running-configuration file, and you can display this file by entering the [show running-config](#) command.

Example

```
Console(config)#vlan database
Console(config-vlan)#
```

Related Commands

[show vlan \(492\)](#)

vlan This command configures a VLAN. Use the **no** form to restore the default settings or delete a VLAN.

Syntax

vlan *vlan-id* [**name** *vlan-name*] **media ethernet**
[**state** {**active** | **suspend**}] [**rspan**]

no vlan *vlan-id* [**name** | **state**]

vlan-id - VLAN ID, specified as a single number, a range of consecutive numbers separated by a hyphen, or multiple numbers separated by commas. (Range: 1-4094)

name - Keyword to be followed by the VLAN name.

vlan-name - ASCII string from 1 to 32 characters.

media ethernet - Ethernet media type.

state - Keyword to be followed by the VLAN state.

active - VLAN is operational.

suspend - VLAN is suspended. Suspended VLANs do not pass packets.

rspan - Keyword to create a VLAN used for mirroring traffic from remote switches. The VLAN used for RSPAN cannot include VLAN 1 (the switch's default VLAN). Nor should it include VLAN 4093 (which is used for switch clustering). Configuring VLAN 4093 for other purposes may cause problems in the Clustering operation. For more information on configuring RSPAN through the CLI, see ["RSPAN Mirroring Commands" on page 417](#).

Default Setting

By default only VLAN 1 exists and is active.

Command Mode

VLAN Database Configuration

Command Usage

- ◆ **no vlan** *vlan-id* deletes the VLAN.
- ◆ **no vlan** *vlan-id* **name** removes the VLAN name.
- ◆ **no vlan** *vlan-id* **state** returns the VLAN to the default state (i.e., active).
- ◆ You can configure up to 4094 VLANs on the switch.

Example

The following example adds a VLAN, using VLAN ID 105 and name RD5. The VLAN is activated by default.

```
Console(config)#vlan database
Console(config-vlan)#vlan 105 name RD5 media ethernet
Console(config-vlan)#
```

Related Commands

[show vlan \(492\)](#)

Configuring VLAN Interfaces

Table 95: Commands for Configuring VLAN Interfaces

Command	Function	Mode
interface vlan	Enters interface configuration mode for a specified VLAN	IC
switchport acceptable-frame-types	Configures frame types to be accepted by an interface	IC
switchport allowed vlan	Configures the VLANs associated with an interface	IC
switchport forbidden vlan	Configures forbidden VLANs for an interface	IC
switchport gvrp	Enables GVRP for an interface	IC
switchport ingress-filtering	Enables ingress filtering on an interface	IC
switchport mode	Configures VLAN membership mode for an interface	IC
switchport native vlan	Configures the PVID (native VLAN) of an interface	IC
switchport priority default	Sets a port priority for incoming untagged frames	IC
vlan-trunking	Allows unknown VLANs to cross the switch	IC

interface vlan This command enters interface configuration mode for VLANs, which is used to configure VLAN parameters for a physical interface.

Syntax

[no] interface vlan *vlan-id*

vlan-id - ID of the configured VLAN. (Range: 1-4094)

Default Setting

None

Command Mode

Global Configuration

Example

The following example shows how to set the interface configuration mode to VLAN 1, and then assign an IP address to the VLAN:

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.254 255.255.255.0
Console(config-if)#
```

Related Commands

[shutdown \(376\)](#)

[interface \(370\)](#)

[vlan \(485\)](#)

switchport acceptable-frame-types This command configures the acceptable frame types for a port. Use the **no** form to restore the default.

Syntax

switchport acceptable-frame-types {all | tagged}

no switchport acceptable-frame-types

all - The port accepts all frames, tagged or untagged.

tagged - The port only receives tagged frames.

Default Setting

All frame types

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN.

Example

The following example shows how to restrict the traffic received on port 1 to tagged frames:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#
```

Related Commands

[switchport mode \(489\)](#)

switchport allowed vlan This command configures VLAN groups on the selected interface. Use the **no** form to restore the default.

Syntax

switchport allowed vlan {**add** *vlan-list* [**tagged** | **untagged**] |
remove *vlan-list*}

no switchport allowed vlan

add *vlan-list* - List of VLAN identifiers to add.

remove *vlan-list* - List of VLAN identifiers to remove.

vlan-list - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. (Range: 1-4094).

Default Setting

All ports are assigned to VLAN 1 by default.
The default frame type is untagged.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ A port, or a trunk with switchport mode set to **hybrid**, must be assigned to at least one VLAN as untagged.
- ◆ If a trunk has switchport mode set to **trunk** (i.e., 1Q Trunk), then you can only assign an interface to VLAN groups as a tagged member.
- ◆ Frames are always tagged within the switch. The tagged/untagged parameter used when adding a VLAN to an interface tells the switch whether to keep or remove the tag from a frame on egress.
- ◆ If none of the intermediate network devices nor the host at the other end of the connection supports VLANs, the interface should be added to these VLANs as an untagged member. Otherwise, it is only necessary to add at most one VLAN as untagged, and this should correspond to the native VLAN for the interface.
- ◆ If a VLAN on the forbidden list for an interface is manually added to that interface, the VLAN is automatically removed from the forbidden list for that interface.

Example

The following example shows how to add VLANs 1, 2, 5 and 6 to the allowed list as tagged VLANs for port 1:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 1,2,5,6 tagged
Console(config-if)#
```


switchport ingress-filtering This command enables ingress filtering for an interface. Use the **no** form to restore the default.

Syntax

[no] switchport ingress-filtering

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ Ingress filtering only affects tagged frames.
- ◆ If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports (except for those VLANs explicitly forbidden on this port).
- ◆ If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.
- ◆ Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STA. However, they do affect VLAN dependent BPDU frames, such as GMRP.

Example

The following example shows how to set the interface to port 1 and then enable ingress filtering:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport ingress-filtering
Console(config-if)#
```

switchport mode This command configures the VLAN membership mode for a port. Use the **no** form to restore the default.

Syntax

switchport mode {hybrid | trunk | private-vlan}

no switchport mode

hybrid - Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.

trunk - Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. Note that frames belonging to the port's default VLAN (i.e., associated with the PVID) are also transmitted as tagged frames.

private-vlan - For an explanation of this command see the [switchport mode private-vlan](#) command.

Default Setting

All ports are in hybrid mode with the PVID set to VLAN 1.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

The following shows how to set the configuration mode to port 1, and then set the switchport mode to hybrid:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport mode hybrid
Console(config-if)#
```

Related Commands

[switchport acceptable-frame-types \(487\)](#)

switchport native vlan This command configures the PVID (i.e., default VLAN ID) for a port. Use the **no** form to restore the default.

Syntax

switchport native vlan *vlan-id*

no switchport native vlan

vlan-id - Default VLAN ID for a port. (Range: 1-4094)

Default Setting

VLAN 1

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ When using Access mode, and an interface is assigned to a new VLAN, its PVID is automatically set to the identifier for that VLAN. When using Hybrid mode, the PVID for an interface can be set to any VLAN for which it is an untagged member.
- ◆ If acceptable frame types is set to **all** or switchport mode is set to **hybrid**, the PVID will be inserted into all untagged frames entering the ingress port.

Example

The following example shows how to set the PVID for port 1 to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport native vlan 3
Console(config-if)#
```

vlan-trunking This command allows unknown VLAN groups to pass through the specified interface. Use the **no** form to disable this feature.

Syntax

[no] vlan-trunking

Default Setting

Disabled

Command Mode

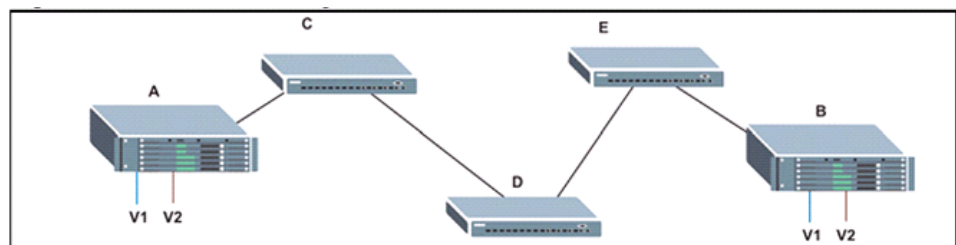
Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ Use this command to configure a tunnel across one or more intermediate switches which pass traffic for VLAN groups to which they do not belong.

The following figure shows VLANs 1 and 2 configured on switches A and B, with VLAN trunking being used to pass traffic for these VLAN groups across switches C, D and E.

Figure 3: Configuring VLAN Trunking



Without VLAN trunking, you would have to configure VLANs 1 and 2 on all intermediate switches – C, D and E; otherwise these switches would drop any frames with unknown VLAN group tags. However, by enabling VLAN trunking on the intermediate switch ports along the path connecting VLANs 1 and 2, you only need to create these VLAN groups in switches A and B. Switches C, D and E automatically allow frames with VLAN group tags 1 and 2 (groups that are unknown to those switches) to pass through their VLAN trunking ports.

- ◆ To prevent loops from forming in the spanning tree, all unknown VLANs will be bound to a single instance (either STP/RSTP or an MSTP instance, depending on the selected STA mode).

- ◆ If both VLAN trunking and ingress filtering are disabled on an interface, packets with unknown VLAN tags will still be allowed to enter this interface and will be flooded to all other ports where VLAN trunking is enabled. (In other words, VLAN trunking will still be effectively enabled for the unknown VLAN).

Example

The following example enables VLAN trunking on ports 9 and 10 to establish a path across the switch for unknown VLAN groups:

```
Console(config)#interface ethernet 1/9
Console(config-if)#vlan-trunking
Console(config-if)#interface ethernet 1/10
Console(config-if)#vlan-trunking
Console(config-if)#
```

Displaying VLAN Information

This section describes commands used to display VLAN information.

Table 96: Commands for Displaying VLAN Information

Command	Function	Mode
<code>show interfaces status vlan</code>	Displays status for the specified VLAN interface	NE, PE
<code>show interfaces switchport</code>	Displays the administrative and operational status of an interface	NE, PE
<code>show vlan</code>	Shows VLAN information	NE, PE

show vlan This command shows VLAN information.

Syntax

show vlan [**id** *vlan-id* | **name** *vlan-name*]

id - Keyword to be followed by the VLAN ID.

vlan-id - ID of the configured VLAN. (Range: 1-4094)

name - Keyword to be followed by the VLAN name.

vlan-name - ASCII string from 1 to 32 characters.

Default Setting

Shows all VLANs.

Command Mode

Normal Exec, Privileged Exec

Example

The following example shows how to display information for VLAN 1:

```
Console#show vlan id 1

VLAN ID          : 1
Type              : Static
Name              : DefaultVlan
Status            : Active
Ports/Port Channels : Eth1/ 1(S) Eth1/ 2(S) Eth1/ 3(S) Eth1/ 4(S) Eth1/ 5(S)
                    Eth1/ 6(S) Eth1/ 7(S) Eth1/ 8(S) Eth1/ 9(S) Eth1/10(S)
                    Eth1/11(S) Eth1/12(S) Eth1/13(S) Eth1/14(S) Eth1/15(S)
                    Eth1/16(S) Eth1/17(S) Eth1/18(S) Eth1/19(S) Eth1/20(S)
                    Eth1/21(S) Eth1/22(S) Eth1/23(S) Eth1/24(S) Eth1/25(S)
                    Eth1/26(S) Eth1/27(S) Eth1/28(S) Eth1/29(S) Eth1/30(S)
                    Eth1/31(S) Eth1/32(S) Eth1/33(S) Eth1/34(S) Eth1/35(S)
                    Eth1/36(S) Eth1/37(S) Eth1/38(S) Eth1/39(S) Eth1/40(S)
                    Eth1/41(S) Eth1/42(S) Eth1/43(S) Eth1/44(S) Eth1/45(S)
                    Eth1/46(S) Eth1/47(S) Eth1/48(S) Eth1/49(S) Eth1/50(S)
                    Eth1/51(S) Eth1/52(S)
```

```
Console#
```

Configuring IEEE 802.1Q Tunneling

IEEE 802.1Q tunneling (QinQ tunneling) uses a single Service Provider VLAN (SPVLAN) for customers who have multiple VLANs. Customer VLAN IDs are preserved and traffic from different customers is segregated within the service provider's network even when they use the same customer-specific VLAN IDs. QinQ tunneling expands VLAN space by using a VLAN-in-VLAN hierarchy, preserving the customer's original tagged packets, and adding SPVLAN tags to each frame (also called double tagging).

This section describes commands used to configure QinQ tunneling.

Table 97: 802.1Q Tunneling Commands

Command	Function	Mode
<code>dot1q-tunnel system-tunnel-control</code>	Configures the switch to operate in normal mode or QinQ mode	GC
<code>switchport dot1q-tunnel mode</code>	Configures an interface as a QinQ tunnel port	IC
<code>switchport dot1q-tunnel service match cvlan</code>	Creates a CVLAN to SPVLAN mapping entry	IC
<code>switchport dot1q-tunnel tpid</code>	Sets the Tag Protocol Identifier (TPID) value of a tunnel port	IC
<code>show dot1q-tunnel</code>	Displays the configuration of QinQ tunnel ports	PE
<code>show interfaces switchport</code>	Displays port QinQ operational status	PE

General Configuration Guidelines for QinQ

1. Configure the switch to QinQ mode (`dot1q-tunnel system-tunnel-control`).
2. Create a SPVLAN (`vlan`).
3. Configure the QinQ tunnel access port to dot1Q-tunnel access mode (`switchport dot1q-tunnel mode`).
4. Set the Tag Protocol Identifier (TPID) value of the tunnel access port. This step is required if the attached client is using a nonstandard 2-byte ethertype to identify 802.1Q tagged frames. The standard ethertype value is 0x8100. (See `switchport dot1q-tunnel tpid`.)
5. Configure the QinQ tunnel access port to join the SPVLAN as an untagged member (`switchport allowed vlan`).
6. Configure the SPVLAN ID as the native VID on the QinQ tunnel access port (`switchport native vlan`).
7. Configure the QinQ tunnel uplink port to dot1Q-tunnel uplink mode (`switchport dot1q-tunnel mode`).
8. Configure the QinQ tunnel uplink port to join the SPVLAN as a tagged member (`switchport allowed vlan`).

Limitations for QinQ

- ◆ The native VLAN for the tunnel uplink ports and tunnel access ports cannot be the same. However, the same service VLANs can be set on both tunnel port types.
- ◆ IGMP Snooping should not be enabled on a tunnel access port.
- ◆ If the spanning tree protocol is enabled, be aware that a tunnel access or tunnel uplink port may be disabled if the spanning tree structure is automatically reconfigured to overcome a break in the tree. It is therefore advisable to disable spanning tree on these ports.

dot1q-tunnel system-tunnel-control This command sets the switch to operate in QinQ mode. Use the **no** form to disable QinQ operating mode.

Syntax

[no] dot1q-tunnel system-tunnel-control

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

QinQ tunnel mode must be enabled on the switch for QinQ interface settings to be functional.

Example

```
Console(config)#dot1q-tunnel system-tunnel-control  
Console(config)#
```

Related Commands

[show dot1q-tunnel \(499\)](#)

[show interfaces switchport \(394\)](#)

switchport dot1q-tunnel mode This command configures an interface as a QinQ tunnel port. Use the **no** form to disable QinQ on the interface.

Syntax

switchport dot1q-tunnel mode {access | uplink}

no switchport dot1q-tunnel mode

access – Sets the port as an 802.1Q tunnel access port.

uplink – Sets the port as an 802.1Q tunnel uplink port.

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ QinQ tunneling must be enabled on the switch using the [dot1q-tunnel system-tunnel-control](#) command before the **switchport dot1q-tunnel mode** interface command can take effect.
- ◆ When a tunnel uplink port receives a packet from a customer, the customer tag (regardless of whether there are one or more tag layers) is retained in the inner tag, and the service provider's tag added to the outer tag.
- ◆ When a tunnel uplink port receives a packet from the service provider, the outer service provider's tag is stripped off, and the packet passed on to the VLAN indicated by the inner tag. If no inner tag is found, the packet is passed onto the native VLAN defined for the uplink port.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel mode access
Console(config-if)#
```

Related Commands

[show dot1q-tunnel \(499\)](#)

[show interfaces switchport \(394\)](#)

switchport dot1q-tunnel service match cvid

This command creates a CVLAN to SPVLAN mapping entry. Use the **no** form to delete a VLAN mapping entry.

Syntax

switchport dot1q-tunnel service *svid* match cvid *cvid* [remove-ctag]

svid - VLAN ID for the outer VLAN tag (Service Provider VID). (Range: 1-4094)

cvid - VLAN ID for the inner VLAN tag (Customer VID). (Range: 1-4094)

remove-ctag - Removes the customer's VLAN tag.

Default Setting

Default mapping uses the PVID of the ingress port on the edge router for the SPVID.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ The inner VLAN tag of a customer packet entering the edge router of a service provider's network is mapped to an outer tag indicating the service provider VLAN that will carry this traffic across the 802.1Q tunnel. This process is performed in a transparent manner.
- ◆ When priority bits are found in the inner tag, these are also copied to the outer tag. This allows the service provider to differentiate service based on the indicated priority and appropriate methods of queue management at intermediate nodes across the tunnel.
- ◆ Rather than relying on standard service paths and priority queuing, QinQ VLAN mapping can be used to further enhance service by defining a set of differentiated service pathways to follow across the service provider's network for traffic arriving from specified inbound customer VLANs.
- ◆ Note that all customer interfaces should be configured as access interfaces (that is, a user-to-network interface) and service provider interfaces as uplink interfaces (that is, a network-to-network interface). Use the [switchport dot1q-tunnel mode uplink](#) command to set an interface to access or uplink mode.

- ◆ When the **remove-ctag** option is specified, the inner-tag containing the customer's VID is removed, and the outer-tag containing the service provider's VID remains in place.

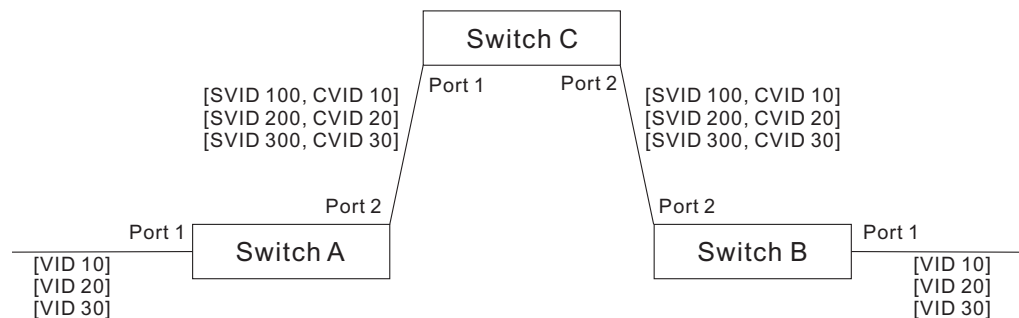
Example

This example sets the SVID to 99 in the outer tag for egress packets exiting port 1 when the packet's CVID is 2.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel service 99 match cvid 2
Console(config-if)#
```

The following example maps C-VLAN 10 to S-VLAN 100, C-VLAN 20 to S-VLAN 200 and C-VLAN 30 to S-VLAN 300 for ingress traffic on port 1 of Switches A and B.

Figure 4: Mapping QinQ Service VLAN to Customer VLAN



Step 1. Configure Switch A and B.

1. Create VLANs 100, 200 and 300.

```
Console(config)#vlan database
Console(config-vlan)#vlan 100,200,300 media ethernet state active
```

2. Enable QinQ.

```
Console(config)#dot1q-tunnel system-tunnel-control
```

3. Configure port 2 as a tagged member of VLANs 100, 200 and 300 using uplink mode.

```
Console(config)#interface ethernet 1/2
Console(config-if)#switchport allowed vlan add 100,200,300 tagged
Console(config-if)#switchport dot1q-tunnel mode uplink
```

4. Configures port 1 as an untagged member of VLANs 100, 200 and 300 using access mode.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 100,200,300 untagged
Console(config-if)#switchport dot1q-tunnel mode access
```

5. Configure the following selective QinQ mapping entries.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel service 100 match cvid 10
Console(config-if)#switchport dot1q-tunnel service 200 match cvid 20
```

```
Console(config-if)#switchport dot1q-tunnel service 300 match cvid 30
```

6. Configures port 1 as member of VLANs 10, 20 and 30 to avoid filtering out incoming frames tagged with VID 10, 20 or 30 on port 1

```
Console(config)#interface ethernet 1/1  
Console(config-if)#switchport allowed vlan add 10,20,30
```

7. Verify configuration settings.

```
Console#show dot1q-tunnel service  
802.1Q Tunnel Service Subscriptions
```

Port	Match	C-VID	S-VID
Eth 1/ 1		10	100
Eth 1/ 1		20	200
Eth 1/ 1		30	300

Step 2. Configure Switch C.

1. Create VLAN 100, 200 and 300.

```
Console(config)#vlan database  
Console(config-vlan)#vlan 100,200,300 media ethernet state active
```

2. Configure port 1 and port 2 as tagged members of VLAN 100, 200 and 300.

```
Console(config)#interface ethernet 1/1,2  
Console(config-if)#switchport allowed vlan add 100,200,300 tagged
```

switchport dot1q-tunnel tpid This command sets the Tag Protocol Identifier (TPID) value of a tunnel port. Use the **no** form to restore the default setting.

Syntax

switchport dot1q-tunnel tpid *tpid*

no switchport dot1q-tunnel tpid

tpid – Sets the ethertype value for 802.1Q encapsulation. This identifier is used to select a nonstandard 2-byte ethertype to identify 802.1Q tagged frames. The standard ethertype value is 0x8100. (Range: 0800-FFFF hexadecimal)

Default Setting

0x8100

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ Use the **switchport dot1q-tunnel tpid** command to set a custom 802.1Q ethertype value on the selected interface. This feature allows the switch to interoperate with third-party switches that do not use the standard 0x8100 ethertype to identify 802.1Q-tagged frames. For example, 0x1234 is set as the custom 802.1Q ethertype on a trunk port, incoming frames containing that

ethertype are assigned to the VLAN contained in the tag following the ethertype field, as they would be with a standard 802.1Q trunk. Frames arriving on the port containing any other ethertype are looked upon as untagged frames, and assigned to the native VLAN of that port.

- ◆ The specified ethertype only applies to ports configured in Uplink mode using the `switchport dot1q-tunnel mode` command. If the port is in normal mode, the TPID is always 8100. If the port is in Access mode, received packets are processes as untagged packets.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel tpid 9100
Console(config-if)#
```

Related Commands

[show interfaces switchport \(394\)](#)

show dot1q-tunnel This command displays information about QinQ tunnel ports.

Syntax

show dot1q-tunnel [**interface** *interface* [**service** *svid*] | **service** [*svid*]]

interface

ethernet *unit/port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

svid - VLAN ID for the outer VLAN tag (SPVID). (Range: 1-4094)

Command Mode

Privileged Exec

Example

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel mode access
Console(config-if)#interface ethernet 1/2
Console(config-if)#switchport dot1q-tunnel mode uplink
Console(config-if)#end
Console#show dot1q-tunnel
802.1Q Tunnel Status : Enabled
```

Port	Mode	TPID (hex)
Eth 1/ 1	Access	8100
Eth 1/ 2	Uplink	8100
Eth 1/ 3	Normal	8100
:		

```
Console#show dot1q-tunnel interface ethernet 1/5
802.1Q Tunnel Service Subscriptions

Port      Match C-VID S-VID Remove C-Tag
-----
Eth 1/ 5          1   100 Disabled

Console#show dot1q-tunnel service 100
802.1Q Tunnel Service Subscriptions

Port      Match C-VID S-VID Remove C-Tag
-----
Eth 1/ 5          1   100 Disabled
Eth 1/ 6          1   100 Enabled

Console#
```

Related Commands

[switchport dot1q-tunnel mode \(495\)](#)

Configuring L2CP Tunneling

This section describes the commands used to configure Layer 2 Protocol Tunneling (L2PT).

Table 98: L2 Protocol Tunnel Commands

Command	Function	Mode
l2protocol-tunnel tunnel-dmac	Configures the destination address for Layer 2 Protocol Tunneling	GC
switchport l2protocol-tunnel	Enables Layer 2 Protocol Tunneling for the specified protocol	IC
show l2protocol-tunnel	Shows settings for Layer 2 Protocol Tunneling	PE

[l2protocol-tunnel tunnel-dmac](#) This command configures the destination address for Layer 2 Protocol Tunneling (L2PT). Use the **no** form to restore the default setting.

Syntax

[l2protocol-tunnel tunnel-dmac](#) *mac-address*

mac-address – The switch rewrites the destination MAC address in all upstream L2PT protocol packets (i.e, STP BPDUs) to this value, and forwards them on to uplink ports. The MAC address must be specified in the format **xx-xx-xx-xx-xx-xx** or **xxxxxxxxxxxx**.

Default Setting

01-12-CF-00-00-02, proprietary tunnel address

Command Mode

Global Configuration

Command Usage

- ◆ When L2PT is not used, protocol packets (such as STP) are flooded to 802.1Q access ports on the same edge switch, but filtered from 802.1Q tunnel ports. This creates disconnected protocol domains in the customer's network.
- ◆ L2PT can be used to pass various types of protocol packets belonging to the same customer transparently across a service provider's network. In this way, normally segregated network segments can be configured to function inside a common protocol domain.
- ◆ L2PT encapsulates protocol packets entering ingress ports on the service provider's edge switch, replacing the destination MAC address with a proprietary MAC address (for example, the spanning tree protocol uses 10-12-CF-00-00-02), a reserved address for other specified protocol types (as defined in IEEE 802.1ad – Provider Bridges), or a user-defined address. All intermediate switches carrying this traffic across the service provider's network treat these encapsulated packets in the same way as normal data, forwarding them across to the tunnel's egress port. The egress port decapsulates these packets, restores the proper protocol and MAC address information, and then floods them onto the same VLANs at the customer's remote site (via all of the appropriate tunnel ports and access ports¹¹ connected to the same metro VLAN).
- ◆ The way in which L2PT processes packets is based on the following criteria – (1) packet is received on a QinQ uplink port, (2) packet is received on a QinQ access port, or (3) received packet is Cisco-compatible L2PT (i.e., as indicated by a proprietary MAC address).

Processing protocol packets defined in IEEE 802.1ad – Provider Bridges

- ◆ When an IEEE 802.1ad protocol packet is received on an uplink port (i.e., an 802.1Q tunnel ingress port connecting the edge switch to the service provider network)
 - with the destination address 01-80-C2-00-00-00,0B~0F (C-VLAN tag), it is forwarded to all QinQ uplink ports and QinQ access ports in the same S-VLAN for which L2PT is enabled for that protocol.
 - with the destination address 01-80-C2-00-00-01~0A (S-VLAN tag), it is filtered, decapsulated, and processed locally by the switch if the protocol is supported.

11. Access ports in this context are 802.1Q trunk ports.

- ◆ When a protocol packet is received on an access port (i.e., an 802.1Q trunk port connecting the edge switch to the local customer network)
 - with the destination address 01-80-C2-00-00-00,0B~0F (C-VLAN), and
 - L2PT is enabled on the port, the frame is forwarded to all QinQ uplink ports and QinQ access ports on which L2PT is enabled for that protocol in the same S-VLAN.
 - L2PT is disabled on the port, the frame is decapsulated and processed locally by the switch if the protocol is supported.
 - with destination address 01-80-C2-00-00-01~0A (S-VLAN), the frame is filtered, decapsulated, and processed locally by the switch if the protocol is supported.

Processing Cisco-compatible protocol packets

- ◆ When a Cisco-compatible L2PT packet is received on an uplink port, and
 - recognized as a CDP/VTP/STP/PVST+ protocol packet (where STP means STP/RSTP/MSTP), it is forwarded to the following ports in the same S-VLAN: (a) all access ports for which L2PT has been disabled, and (b) all uplink ports.
 - recognized as a Generic Bridge PDU Tunneling (GBPT) protocol packet (i.e., having the destination address 01-00-0C-CD-CD-D0), it is forwarded to the following ports in the same S-VLAN:
 - other access ports for which L2PT is enabled after decapsulating the packet and restoring the proper protocol and MAC address information.
 - all uplink ports.
- ◆ When a Cisco-compatible L2PT packet is received on an access port, and
 - recognized as a CDP/VTP/STP/PVST+ protocol packet, and
 - L2PT is enabled on this port, it is forwarded to the following ports in the same S-VLAN: (a) other access ports for which L2PT is enabled, and (b) uplink ports after rewriting the destination address to make it a GBPT protocol packet (i.e., setting the destination address to 01-00-0C-CD-CD-D0).
 - L2PT is disabled on this port, it is forwarded to the following ports in the same S-VLAN: (a) other access ports for which L2PT is disabled, and (b) all uplink ports.
 - recognized as a GBPT protocol packet (i.e., having the destination address 01-00-0C-CD-CD-D0), and
 - L2PT is enabled on this port, it is forwarded to other access ports in the same S-VLAN for which L2PT is enabled

- L2PT is disabled on this port, it is forwarded to the following ports in the same S-VLAN: (a) other access ports for which L2PT is disabled, and (b) all uplink ports.
- ◆ For L2PT to function properly, QinQ must be enabled on the switch using the `dot1q-tunnel system-tunnel-control` command, and the interface configured to 802.1Q tunnel mode using the `switchport dot1q-tunnel mode` command.

Example

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#l2protocol-tunnel tunnel-dmac 01-80-C2-00-00-01
Console(config-)#
```

switchport l2protocol-tunnel This command enables Layer 2 Protocol Tunneling (L2PT) for the specified protocol. Use the **no** form to disable L2PT for the specified protocol.

Syntax

switchport l2protocol-tunnel {cdp | lldp | pvst+ | spanning-tree | vtp}

cdp - Cisco Discovery Protocol

lldp - Link Layer Discovery Protocol

pvst+ - Cisco Per VLAN Spanning Tree Plus

spanning-tree - Spanning Tree (STP, RSTP, MSTP)

vtp - Cisco VLAN Trunking Protocol

Default Setting

Disabled for all protocols

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ Refer to the Command Usage section for the `l2protocol-tunnel tunnel-dmac` command.
- ◆ For L2PT to function properly, QinQ must be enabled on the switch using the `dot1q-tunnel system-tunnel-control` command, and the interface configured to 802.1Q tunnel mode using the `switchport dot1q-tunnel mode` command.

Example

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel mode access
Console(config-if)#switchport l2protocol-tunnel spanning-tree
Console(config-if)#
```

show l2protocol-tunnel This command shows settings for Layer 2 Protocol Tunneling (L2PT).

Command Mode
Privileged Exec

Example

```
Console#show l2protocol-tunnel
Layer 2 Protocol Tunnel

Tunnel MAC Address : 01-12-CF-00-00-00

Interface  Protocol
-----
Eth 1/ 1   Spanning Tree

Console#
```

Configuring VLAN Translation

QinQ tunneling uses double tagging to preserve the customer's VLAN tags on traffic crossing the service provider's network. However, if any switch in the path crossing the service provider's network does not support this feature, then the switches directly connected to that device can be configured to swap the customer's VLAN ID with the service provider's VLAN ID for upstream traffic, or the service provider's VLAN ID with the customer's VLAN ID for downstream traffic.

This section describes commands used to configure VLAN translation.

Table 99: VLAN Translation Commands

Command	Function	Mode
switchport vlan-translation	Maps VLAN IDs between the customer and service provider	IC
show vlan-translation	Displays the configuration settings for VLAN translation	PE

switchport vlan-translation This command maps VLAN IDs between the customer and service provider.

Syntax

switchport vlan-translation *original-vlan new-vlan*

no switchport vlan-translation *original-vlan*

original-vlan - The original VLAN ID. (Range: 1-4094)

new-vlan - The new VLAN ID. (Range: 1-4094)

Default Setting

Disabled

Command Mode

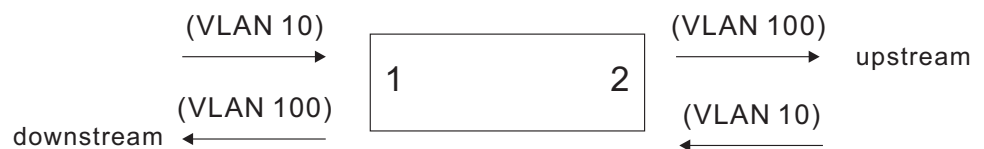
Interface Configuration (Ethernet)

Command Usage

- ◆ If the next switch upstream does not support QinQ tunneling, then use this command to map the customer's VLAN ID to the service provider's VLAN ID for the upstream port. Similarly, if the next switch downstream does not support QinQ tunneling, then use this command to map the service provider's VLAN ID to the customer's VLAN ID for the downstream port. Note that one command maps both the *original-vlan* to *new-vlan* for ingress traffic and the *new-vlan* to *original-vlan* for egress traffic on the specified port.

For example, assume that the upstream switch does not support QinQ tunneling. If the command **switchport vlan-translation 10 100** is used to map VLAN 10 to VLAN 100 for upstream traffic entering port 1, and VLAN 100 to VLAN 10 for downstream traffic leaving port 1, then the VLAN IDs will be swapped as shown below.

Figure 5: Configuring VLAN Translation



- ◆ The maximum number of VLAN translation entries is 8 per port, and up to 96 for the system. However, note that configuring a large number of entries may degrade the performance of other processes that also use the TCAM, such as IP Source Guard filter rules, Quality of Service (QoS) processes, QinQ, MAC-based VLANs, VLAN translation, or traps.
- ◆ If VLAN translation is set on an interface with this command, and the same interface is also configured as a QinQ access port with the [switchport dot1q-tunnel mode](#) command, VLAN tag assignments will be determined by the QinQ process, not by VLAN translation.

Example

This example configures VLAN translation for Port 1 as described in the Command Usage section above.

```
Console(config)#vlan database
Console(config-vlan)#vlan 10 media ethernet state active
Console(config-vlan)#vlan 100 media ethernet state active
Console(config-vlan)#exit
Console(config)#interface ethernet 1/1,2
Console(config-if)#switchport allowed vlan add 10 tagged
Console(config-if)#switchport allowed vlan add 100 tagged
Console(config-if)#interface ethernet 1/1
Console(config-if)#switchport vlan-translation 10 100
Console(config-if)#end
Console#show vlan-translation
```

```
Interface Old VID New VID
-----
Eth 1/ 1      10    100

Console#
```

show vlan-translation This command displays the configuration settings for VLAN translation.

Syntax

show vlan-translation [**interface** *interface*]

interface

ethernet *unit/port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-52)

Command Mode

Privileged Exec

Example

```
Console#show vlan-translation

Interface Old VID New VID
-----
Eth 1/ 1      10    100

Console#
```

Configuring Private VLANs

Private VLANs provide port-based security and isolation of local ports contained within different private VLAN groups. This switch supports two types of private VLANs – primary and community groups. A primary VLAN contains promiscuous ports that can communicate with all other ports in the associated private VLAN groups, while a community (or secondary) VLAN contains community ports that can only communicate with other hosts within the community VLAN and with any of the promiscuous ports in the associated primary VLAN. The promiscuous ports are designed to provide open access to an external network such as the Internet, while the community ports provide restricted access to local users.

Multiple primary VLANs can be configured on this switch, and multiple community VLANs can be associated with each primary VLAN. (Note that private VLANs and normal VLANs can exist simultaneously within the same switch.)

This section describes commands used to configure private VLANs.

Table 100: Private VLAN Commands

Command	Function	Mode
<i>Edit Private VLAN Groups</i>		
<code>private-vlan</code>	Adds or deletes primary or community VLANs	VC
<code>private vlan association</code>	Associates a community VLAN with a primary VLAN	VC
<i>Configure Private VLAN Interfaces</i>		
<code>switchport mode private-vlan</code>	Sets an interface to host mode or promiscuous mode	IC
<code>switchport private-vlan host-association</code>	Associates an interface with a secondary VLAN	IC
<code>switchport private-vlan mapping</code>	Maps an interface to a primary VLAN	IC
<i>Display Private VLAN Information</i>		
<code>show vlan private-vlan</code>	Shows private VLAN information	NE, PE

To configure private VLANs, follow these steps:

1. Use the `private-vlan` command to designate one or more community VLANs and the primary VLAN that will channel traffic outside of the community groups.
2. Use the `private vlan association` command to map the community VLAN(s) to the primary VLAN.
3. Use the `switchport mode private-vlan` command to configure ports as promiscuous (i.e., having access to all ports in the primary VLAN) or host (i.e., community port).
4. Use the `switchport private-vlan host-association` command to assign a port to a community VLAN.
5. Use the `switchport private-vlan mapping` command to assign a port to a primary VLAN.
6. Use the `show vlan private-vlan` command to verify your configuration settings.

private-vlan Use this command to create a primary or community private VLAN. Use the **no** form to remove the specified private VLAN.

Syntax

private-vlan *vlan-id* {**community** | **primary**}

no private-vlan *vlan-id*

vlan-id - ID of private VLAN. (Range: 1-4094)

community - A VLAN in which traffic is restricted to host members in the same VLAN and to promiscuous ports in the associate primary VLAN.

primary - A VLAN which can contain one or more community VLANs, and serves to channel traffic between community VLANs and other locations.

Default Setting

None

Command Mode

VLAN Configuration

Command Usage

- ◆ Private VLANs are used to restrict traffic to ports within the same community, and channel traffic passing outside the community through promiscuous ports. When using community VLANs, they must be mapped to an associated "primary" VLAN that contains promiscuous ports.
- ◆ Port membership for private VLANs is static. Once a port has been assigned to a private VLAN, it cannot be dynamically moved to another VLAN via GVRP.
- ◆ Private VLAN ports cannot be set to trunked mode. (See ["switchport mode" on page 489.](#))

Example

```
Console(config)#vlan database
Console(config-vlan)#private-vlan 2 primary
Console(config-vlan)#private-vlan 3 community
Console(config)#
```

private-vlan association Use this command to associate a primary VLAN with a secondary (i.e., community) VLAN. Use the **no** form to remove all associations for the specified primary VLAN.

Syntax

private-vlan *primary-vlan-id* **association** [*secondary-vlan-id* |
add *secondary-vlan-id* | **remove** *secondary-vlan-id*]

no private-vlan *primary-vlan-id* **association**

primary-vlan-id - ID of primary VLAN. (Range: 1-4094)

secondary-vlan-id - ID of secondary (i.e, community) VLAN.
(Range: 1-4094)

Default Setting

None

Command Mode

VLAN Configuration

Command Usage

Secondary VLANs provide security for group members. The associated primary VLAN provides a common interface for access to other network resources within the primary VLAN (e.g., servers configured with promiscuous ports) and to resources outside of the primary VLAN (via promiscuous ports).

Example

```
Console(config-vlan)#private-vlan 2 association 3
Console(config)#
```

switchport mode private-vlan Use this command to set the private VLAN mode for an interface. Use the **no** form to restore the default setting.

Syntax

switchport mode private-vlan {**host** | **promiscuous**}

no switchport mode private-vlan

host – This port type can subsequently be assigned to a community VLAN.

promiscuous – This port type can communicate with all other promiscuous ports in the same primary VLAN, as well as with all the ports in the associated secondary VLANs.

Default Setting

Normal VLAN

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

To assign a promiscuous port to a primary VLAN, use the [switchport private-vlan mapping](#) command. To assign a host port to a community VLAN, use the [switchport private-vlan host-association](#) command.

Example

```
Console(config)#interface ethernet 1/2
Console(config-if)#switchport mode private-vlan promiscuous
Console(config-if)#exit
Console(config)#interface ethernet 1/3
Console(config-if)#switchport mode private-vlan host
Console(config-if)#
```

switchport private-vlan host-association

Use this command to associate an interface with a secondary VLAN. Use the **no** form to remove this association.

Syntax

switchport private-vlan host-association *secondary-vlan-id*

no switchport private-vlan host-association

secondary-vlan-id - ID of secondary (i.e., community) VLAN. (Range: 1-4094)

Default Setting

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

All ports assigned to a secondary (i.e., community) VLAN can pass traffic between group members, but must communicate with resources outside of the group via promiscuous ports in the associated primary VLAN.

Example

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport private-vlan host-association 3
Console(config-if)#
```

switchport private-vlan mapping Use this command to map an interface to a primary VLAN. Use the **no** form to remove this mapping.

Syntax

switchport private-vlan mapping *primary-vlan-id*

no switchport private-vlan mapping

primary-vlan-id – ID of primary VLAN. (Range: 1-4094)

Default Setting

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

Promiscuous ports assigned to a primary VLAN can communicate with any other promiscuous ports in the same VLAN, and with the group members within any associated secondary VLANs.

Example

```
Console(config)#interface ethernet 1/2
Console(config-if)#switchport private-vlan mapping 2
Console(config-if)#
```

show vlan private-vlan Use this command to show the private VLAN configuration settings on this switch.

Syntax

show vlan private-vlan [**community** | **primary**]

community – Displays all community VLANs, along with their associated primary VLAN and assigned host interfaces.

primary – Displays all primary VLANs, along with any assigned promiscuous interfaces.

Default Setting

None

Command Mode

Privileged Executive

Example

```
Console#show vlan private-vlan
Primary   Secondary   Type         Interfaces
-----
          5              primary      Eth1/ 3
```

```
5          6          community   Eth1/ 4 Eth1/ 5
Console#
```

Configuring Protocol-based VLANs

The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of the basic benefits of VLANs, including security and easy accessibility.

To avoid these problems, you can configure this switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type in use by the inbound packets.

Table 101: Protocol-based VLAN Commands

Command	Function	Mode
<code>protocol-vlan protocol-group</code>	Create a protocol group, specifying the supported protocols	GC
<code>protocol-vlan protocol-group</code>	Maps a protocol group to a VLAN	IC
<code>show protocol-vlan protocol-group</code>	Shows the configuration of protocol groups	PE
<code>show interfaces protocol-vlan protocol-group</code>	Shows the interfaces mapped to a protocol group and the corresponding VLAN	PE

To configure protocol-based VLANs, follow these steps:

1. First configure VLAN groups for the protocols you want to use ([page 485](#)). Although not mandatory, we suggest configuring a separate VLAN for each major protocol running on your network. Do not add port members at this time.
2. Create a protocol group for each of the protocols you want to assign to a VLAN using the `protocol-vlan protocol-group` command (Global Configuration mode).
3. Then map the protocol for each interface to the appropriate VLAN using the `protocol-vlan protocol-group` command (Interface Configuration mode).

protocol-vlan
protocol-group
(Configuring Groups)

This command creates a protocol group, or to add specific protocols to a group. Use the **no** form to remove a protocol group.

Syntax

protocol-vlan protocol-group *group-id* [{**add** | **remove**}
frame-type *frame* **protocol-type** *protocol*]

no protocol-vlan protocol-group *group-id*

group-id - Group identifier of this protocol group. (Range: 1-2147483647)

*frame*¹² - Frame type used by this protocol. (Options: ethernet, rfc_1042, llc_other)

protocol - Protocol type. The only option for the llc_other frame type is ipx_raw. The options for all other frames types include: arp, ip, ipv6, rarp.

Default Setting

No protocol groups are configured.

Command Mode

Global Configuration

Example

The following creates protocol group 1, and specifies Ethernet frames with IP and ARP protocol types:

```
Console(config)#protocol-vlan protocol-group 1 add frame-type ethernet  
protocol-type ip  
Console(config)#protocol-vlan protocol-group 1 add frame-type ethernet  
protocol-type arp  
Console(config)#
```

protocol-vlan
protocol-group
(Configuring
Interfaces)

This command maps a protocol group to a VLAN for the current interface. Use the **no** form to remove the protocol mapping for this interface.

Syntax

protocol-vlan protocol-group *group-id* **vlan** *vlan-id* [**priority** *priority*]

no protocol-vlan protocol-group *group-id* **vlan**

group-id - Group identifier of this protocol group. (Range: 1-2147483647)

vlan-id - VLAN to which matching protocol traffic is forwarded.
(Range: 1-4094)

priority - The priority assigned to untagged ingress traffic. (Range: 0-3, where 3 is the highest priority)

¹². SNAP frame types are not supported by this switch due to hardware limitations.

Default Setting

No protocol groups are mapped for any interface.
Priority: 0

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ When creating a protocol-based VLAN, only assign interfaces via this command. If you assign interfaces using any of the other VLAN commands (such as the `vlan` command), these interfaces will admit traffic of any protocol type into the associated VLAN.
- ◆ When MAC-based, IP subnet-based, and protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.
- ◆ When a frame enters a port that has been assigned to a protocol VLAN, it is processed in the following manner:
 - If the frame is tagged, it will be processed according to the standard rules applied to tagged frames.
 - If the frame is untagged and the protocol type matches, the frame is forwarded to the appropriate VLAN.
 - If the frame is untagged but the protocol type does not match, the frame is forwarded to the default VLAN for this interface.

Example

The following example maps the traffic entering Port 1 which matches the protocol type specified in protocol group 1 to VLAN 2.

```
Console(config)#interface ethernet 1/1
Console(config-if)#protocol-vlan protocol-group 1 vlan 2
Console(config-if)#
```

show protocol-vlan protocol-group

This command shows the frame and protocol type associated with protocol groups.

Syntax

show protocol-vlan protocol-group *[group-id]*

group-id - Group identifier for a protocol group. (Range: 1-2147483647)

Default Setting

All protocol groups are displayed.

Command Mode

Privileged Exec

Example

This shows protocol group 1 configured for IP over Ethernet:

```
Console#show protocol-vlan protocol-group

Protocol Group ID   Frame Type   Protocol Type
-----
                  1      ethernet    08 00
Console#
```

show interfaces protocol-vlan protocol-group

This command shows the mapping from protocol groups to VLANs for the selected interfaces.

Syntax

show interfaces protocol-vlan protocol-group [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Default Setting

The mapping for all interfaces is displayed.

Command Mode

Privileged Exec

Example

This shows that traffic entering Port 1 that matches the specifications for protocol group 1 will be mapped to VLAN 2:

```
Console#show interfaces protocol-vlan protocol-group

Port      Protocol Group ID VLAN ID Priority
-----
Eth 1/ 2 1                      1      0
Console#
```

Configuring IP Subnet VLANs

When using IEEE 802.1Q port-based VLAN classification, all untagged frames received by a port are classified as belonging to the VLAN whose VID (PVID) is associated with that port.

When IP subnet-based VLAN classification is enabled, the source address of untagged ingress frames are checked against the IP subnet-to-VLAN mapping table. If an entry is found for that subnet, these frames are assigned to the VLAN indicated in the entry. If no IP subnet is matched, the untagged frames are classified as belonging to the receiving port's VLAN ID (PVID).

Table 102: IP Subnet VLAN Commands

Command	Function	Mode
<code>subnet-vlan</code>	Defines the IP Subnet VLANs	GC
<code>show subnet-vlan</code>	Displays IP Subnet VLAN settings	PE

subnet-vlan This command configures IP Subnet VLAN assignments. Use the **no** form to remove an IP subnet-to-VLAN assignment.

Syntax

subnet-vlan subnet *ip-address mask* **vlan** *vlan-id* [**priority** *priority*]

no subnet-vlan subnet {*ip-address mask* | **all**}

ip-address – The IP address that defines the subnet. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.

mask – This mask identifies the host address bits of the IP subnet.

vlan-id – VLAN to which matching IP subnet traffic is forwarded.
(Range: 1-4094)

priority – The priority assigned to untagged ingress traffic. (Range: 0-7, where 7 is the highest priority)

Default Setting

Priority: 0

Command Mode

Global Configuration

Command Usage

- ◆ Each IP subnet can be mapped to only one VLAN ID. An IP subnet consists of an IP address and a subnet mask. The specified VLAN need not be an existing VLAN.

- ◆ When an untagged frame is received by a port, the source IP address is checked against the IP subnet-to-VLAN mapping table, and if an entry is found, the corresponding VLAN ID is assigned to the frame. If no mapping is found, the PVID of the receiving port is assigned to the frame.
- ◆ The IP subnet cannot be a broadcast or multicast IP address.
- ◆ When MAC-based, IP subnet-based, and protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.

Example

The following example assigns traffic for the subnet 192.168.12.192, mask 255.255.255.224, to VLAN 4.

```
Console(config)#subnet-vlan subnet 192.168.12.192 255.255.255.224 vlan 4
Console(config)#
```

show subnet-vlan This command displays IP Subnet VLAN assignments.

Command Mode

Privileged Exec

Command Usage

- ◆ Use this command to display subnet-to-VLAN mappings.
- ◆ The last matched entry is used if more than one entry can be matched.

Example

The following example displays all configured IP subnet-based VLANs.

```
Console#show subnet-vlan
IP Address      Mask          VLAN ID  Priority
-----
192.168.12.0    255.255.255.128    1        0
192.168.12.128  255.255.255.192    3        0
192.168.12.192  255.255.255.224    4        0
192.168.12.224  255.255.255.240    5        0
192.168.12.240  255.255.255.248    6        0
192.168.12.248  255.255.255.252    7        0
192.168.12.252  255.255.255.254    8        0
192.168.12.254  255.255.255.255    9        0
192.168.12.255  255.255.255.255   10        0
Console#
```

Configuring MAC Based VLANs

When using IEEE 802.1Q port-based VLAN classification, all untagged frames received by a port are classified as belonging to the VLAN whose VID (PVID) is associated with that port.

When MAC-based VLAN classification is enabled, the source address of untagged ingress frames are checked against the MAC address-to-VLAN mapping table. If an entry is found for that address, these frames are assigned to the VLAN indicated in the entry. If no MAC address is matched, the untagged frames are classified as belonging to the receiving port's VLAN ID (PVID).

Table 103: MAC Based VLAN Commands

Command	Function	Mode
<code>mac-vlan</code>	Defines the IP Subnet VLANs	GC
<code>show mac-vlan</code>	Displays IP Subnet VLAN settings	PE

mac-vlan This command configures MAC address-to-VLAN mapping. Use the **no** form to remove an assignment.

Syntax

mac-vlan mac-address mac-address vlan vlan-id [priority priority]

no mac-vlan mac-address {mac-address | all}

mac-address – The source MAC address to be matched. Configured MAC addresses can only be unicast addresses. The MAC address must be specified in the format xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.

vlan-id – VLAN to which the matching source MAC address traffic is forwarded. (Range: 1-4094)

priority – The priority assigned to untagged ingress traffic. (Range: 0-7, where 7 is the highest priority)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ The MAC-to-VLAN mapping applies to all ports on the switch.
- ◆ Source MAC addresses can be mapped to only one VLAN ID.
- ◆ Configured MAC addresses cannot be broadcast or multicast addresses.

- ◆ When MAC-based, IP subnet-based, and protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.

Example

The following example assigns traffic from source MAC address 00-00-00-11-22-33 to VLAN 10.

```
Console(config)#mac-vlan mac-address 00-00-00-11-22-33 vlan 10
Console(config)#
```

show mac-vlan This command displays MAC address-to-VLAN assignments.

Command Mode

Privileged Exec

Command Usage

Use this command to display MAC address-to-VLAN mappings.

Example

The following example displays all configured MAC address-based VLANs.

```
Console#show mac-vlan
MAC Address      VLAN ID  Priority
-----
00-00-00-11-22-33  10      0
Console#
```

Configuring Voice VLANs

The switch allows you to specify a Voice VLAN for the network and set a CoS priority for the VoIP traffic. VoIP traffic can be detected on switch ports by using the source MAC address of packets, or by using LLDP (IEEE 802.1AB) to discover connected VoIP devices. When VoIP traffic is detected on a configured port, the switch automatically assigns the port to the Voice VLAN. Alternatively, switch ports can be manually configured.

Table 104: Voice VLAN Commands

Command	Function	Mode
voice vlan	Defines the Voice VLAN ID	GC
voice vlan aging	Configures the aging time for Voice VLAN ports	GC
voice vlan mac-address	Configures VoIP device MAC addresses	GC
switchport voice vlan	Sets the Voice VLAN port mode	IC

Table 104: Voice VLAN Commands (Continued)

Command	Function	Mode
<code>switchport voice vlan priority</code>	Sets the VoIP traffic priority for ports	IC
<code>switchport voice vlan rule</code>	Sets the automatic VoIP traffic detection method for ports	IC
<code>switchport voice vlan security</code>	Enables Voice VLAN security on ports	IC
<code>show voice vlan</code>	Displays Voice VLAN settings	PE

voice vlan This command enables VoIP traffic detection and defines the Voice VLAN ID. Use the **no** form to disable the Voice VLAN.

Syntax

voice vlan *voice-vlan-id*

no voice vlan

voice-vlan-id - Specifies the voice VLAN ID. (Range: 1-4094)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ When IP telephony is deployed in an enterprise network, it is recommended to isolate the Voice over IP (VoIP) network traffic from other data traffic. Traffic isolation helps prevent excessive packet delays, packet loss, and jitter, which results in higher voice quality. This is best achieved by assigning all VoIP traffic to a single VLAN.
- ◆ VoIP traffic can be detected on switch ports by using the source MAC address of packets, or by using LLDP (IEEE 802.1AB) to discover connected VoIP devices. When VoIP traffic is detected on a configured port, the switch automatically assigns the port as a tagged member of the Voice VLAN.
- ◆ Only one Voice VLAN is supported and it must already be created on the switch before it can be specified as the Voice VLAN.
- ◆ The Voice VLAN ID cannot be modified when the global auto-detection status is enabled (see the `switchport voice vlan` command).

Example

The following example enables VoIP traffic detection and specifies the Voice VLAN ID as 1234.

```
Console(config)#voice vlan 1234  
Console(config)#
```

voice vlan aging This command sets the Voice VLAN ID time out. Use the **no** form to restore the default.

Syntax

voice vlan aging *minutes*

no voice vlan

minutes - Specifies the port Voice VLAN membership time out.
(Range: 5-43200 minutes)

Default Setting

1440 minutes

Command Mode

Global Configuration

Command Usage

The Voice VLAN aging time is the time after which a port is removed from the Voice VLAN when VoIP traffic is no longer received on the port.

The Remaining Age starts to count down when the OUI's MAC address expires from the MAC address table. Therefore, the MAC address aging time should be added to the overall aging time. For example, if you configure the MAC address table aging time to 30 seconds, and the voice VLAN aging time to 5 minutes, then after 5.5 minutes, a port will be removed from voice VLAN when VoIP traffic is no longer received on the port. Alternatively, if you clear the MAC address table manually, then the switch will also start counting down the voice VLAN aging time.

Example

The following example configures the Voice VLAN aging time as 3000 minutes.

```
Console(config)#voice vlan aging 3000  
Console(config)#
```

voice vlan mac-address This command specifies MAC address ranges to add to the OUI Telephony list. Use the **no** form to remove an entry from the list.

Syntax

voice vlan mac-address *mac-address* **mask** *mask-address*
[**description** *description*]

no voice vlan mac-address *mac-address* **mask** *mask-address*

mac-address - Defines a MAC address OUI that identifies VoIP devices in the network. (For example, 01-23-45-00-00-00)

mask-address - Identifies a range of MAC addresses. (Range: 80-00-00-00-00-00 to FF-FF-FF-FF-FF-FF)

description - User-defined text that identifies the VoIP devices. (Range: 1-32 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ VoIP devices attached to the switch can be identified by the manufacturer's Organizational Unique Identifier (OUI) in the source MAC address of received packets. OUI numbers are assigned to manufacturers and form the first three octets of device MAC addresses. The MAC OUI numbers for VoIP equipment can be configured on the switch so that traffic from these devices is recognized as VoIP.
- ◆ Setting a mask of FF-FF-FF-00-00-00 identifies all devices with the same OUI (the first three octets). Other masks restrict the MAC address range. Setting FF-FF-FF-FF-FF-FF specifies a single MAC address.

Example

The following example adds a MAC OUI to the OUI Telephony list.

```
Console(config)#voice vlan mac-address 00-12-34-56-78-90 mask ff-ff-ff-00-00-00 description A new phone
Console(config)#
```

switchport voice vlan This command specifies the Voice VLAN mode for ports. Use the **no** form to disable the Voice VLAN feature on the port.

Syntax

switchport voice vlan {manual | auto}

no switchport voice vlan

manual - The Voice VLAN feature is enabled on the port, but the port must be manually added to the Voice VLAN.

auto - The port will be added as a tagged member to the Voice VLAN when VoIP traffic is detected on the port.

Default Setting

Disabled

Command Mode

Interface Configuration

Command Usage

When auto is selected, you must select the method to use for detecting VoIP traffic, either OUI or 802.1ab (LLDP) using the [switchport voice vlan rule](#) command. When OUI is selected, be sure to configure the MAC address ranges in the Telephony OUI list using the [voice vlan mac-address](#) command.

Example

The following example sets port 1 to Voice VLAN auto mode.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan auto
Console(config-if)#
```

switchport voice vlan priority This command specifies a CoS priority for VoIP traffic on a port. Use the **no** form to restore the default priority on a port.

Syntax

switchport voice vlan priority *priority-value*

no switchport voice vlan priority

priority-value - The CoS priority value. (Range: 0-6)

Default Setting

6

Command Mode

Interface Configuration

Command Usage

Specifies a CoS priority to apply to the port VoIP traffic on the Voice VLAN. The priority of any received VoIP packet is overwritten with the new priority when the Voice VLAN feature is active for the port.

Example

The following example sets the CoS priority to 5 on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan priority 5
Console(config-if)#
```

switchport voice vlan rule This command selects a method for detecting VoIP traffic on a port. Use the **no** form to disable the detection method on the port.

Syntax

[no] switchport voice vlan rule {oui | lldp}

oui - Traffic from VoIP devices is detected by the Organizationally Unique Identifier (OUI) of the source MAC address.

lldp - Uses LLDP to discover VoIP devices attached to the port.

Default Setting

OUI: Enabled

LLDP: Disabled

Command Mode

Interface Configuration

Command Usage

- ◆ When OUI is selected, be sure to configure the MAC address ranges in the Telephony OUI list (see the [voice vlan mac-address](#) command. MAC address OUI numbers must be configured in the Telephony OUI list so that the switch recognizes the traffic as being from a VoIP device.
- ◆ LLDP checks that the “telephone bit” in the system capability TLV is turned on. See [“LLDP Commands” on page 695](#) for more information on LLDP.

Example

The following example enables the OUI method on port 1 for detecting VoIP traffic.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan rule oui
Console(config-if)#
```

switchport voice vlan security This command enables security filtering for VoIP traffic on a port. Use the **no** form to disable filtering on a port.

Syntax

[no] switchport voice vlan security

Default Setting

Disabled

Command Mode

Interface Configuration

Command Usage

- ◆ Security filtering discards any non-VoIP packets received on the port that are tagged with the voice VLAN ID. VoIP traffic is identified by source MAC addresses configured in the Telephony OUI list, or through LLDP that discovers VoIP devices attached to the switch. Packets received from non-VoIP sources are dropped.
- ◆ When enabled, be sure the MAC address ranges for VoIP devices are configured in the Telephony OUI list ([voice vlan mac-address](#)).

Example

The following example enables security filtering on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan security
Console(config-if)#
```

show voice vlan This command displays the Voice VLAN settings on the switch and the OUI Telephony list.

Syntax

show voice vlan {oui | status}

oui - Displays the OUI Telephony list.

status - Displays the global and port Voice VLAN settings.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show voice vlan status
Global Voice VLAN Status
Voice VLAN Status      : Enabled
Voice VLAN ID          : 1234
Voice VLAN aging time  : 1440 minutes

Voice VLAN Port Summary
Port      Mode      Security Rule      Priority Remaining Age
                                   (minutes)
-----
Eth 1/ 1 Auto      Enabled OUI                6 100
Eth 1/ 2 Disabled Disabled OUI                6 NA
Eth 1/ 3 Manual    Enabled OUI                5 100
Eth 1/ 4 Auto      Enabled OUI                6 100
Eth 1/ 5 Disabled Disabled OUI                6 NA
Eth 1/ 6 Disabled Disabled OUI                6 NA
Eth 1/ 7 Disabled Disabled OUI                6 NA
Eth 1/ 8 Disabled Disabled OUI                6 NA
Eth 1/ 9 Disabled Disabled OUI                6 NA
Eth 1/10 Disabled Disabled OUI                6 NA

Console#show voice vlan oui
OUI Address      Mask      Description
-----
00-12-34-56-78-9A FF-FF-FF-00-00-00 old phones
00-11-22-33-44-55 FF-FF-FF-00-00-00 new phones
00-98-76-54-32-10 FF-FF-FF-FF-FF-FF Chris' phone

Console#
```

Class of Service Commands

The commands described in this section allow you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with eight priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. The default priority can be set for each interface, also the queue service mode and the mapping of frame priority tags to the switch's priority queues can be configured.

Table 105: Priority Commands

Command Group	Function
Priority Commands (Layer 2)	Configures the queue mode, queue weights, and default priority for untagged frames
Priority Commands (Layer 3 and 4)	Sets the default priority processing method (CoS or DSCP), maps priority tags for internal processing, maps values from internal priority table to CoS values used in tagged egress packets for Layer 2 interfaces, maps internal per hop behavior to hardware queues

Priority Commands (Layer 2)

This section describes commands used to configure Layer 2 traffic priority on the switch.

Table 106: Priority Commands (Layer 2)

Command	Function	Mode
<code>queue mode</code>	Sets the queue mode to Weighted Round-Robin (WRR), strict priority, or a combination of strict and weighted queuing	IC
<code>queue weight</code>	Assigns round-robin weights to the priority queues	IC
<code>switchport priority default</code>	Sets a port priority for incoming untagged frames	IC
<code>show interfaces switchport</code>	Displays the administrative and operational status of an interface	PE
<code>show queue mode</code>	Shows the current queue mode	PE
<code>show queue weight</code>	Shows weights assigned to the weighted queues	PE

queue mode This command sets the scheduling mode used for processing each of the class of service (CoS) priority queues. The options include strict priority, Weighted Round-Robin (WRR), or a combination of strict and weighted queuing. Use the **no** form to restore the default value.

Syntax

queue mode {**strict** | **wrr** | **strict-wrr** [*queue-type-list*]}

no queue mode

strict - Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues. This ensures that the highest priority packets are always serviced first, ahead of all other traffic.

wrr - Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights (based on the [queue weight](#) command), and servicing each queue in a round-robin fashion.

strict-wrr - Uses strict or weighted service as specified for each queue.

queue-type-list - Indicates if the queue is a normal or strict type.
(Options: 0 indicates a normal queue, 1 indicates a strict queue)

Default Setting

WRR

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ The switch can be set to service the port queues based on strict priority, WRR, or a combination of strict and weighted queuing.
- ◆ Strict priority requires all traffic in a higher priority queue to be processed before lower priority queues are serviced.
- ◆ Weighted Round Robin (WRR) uses a predefined relative weight for each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing. Use the [queue weight](#) command to assign weights for WRR queuing to the eight priority queues.
- ◆ If Strict and WRR mode is selected, a combination of strict and weighted service is used as specified for each queue. The queues assigned to use strict or WRR priority should be specified using the *queue-type-list* parameter.
- ◆ A weight can be assigned to each of the weighted queues (and thereby to the corresponding traffic priorities). This weight sets the frequency at which each queue is polled for service, and subsequently affects the response time for software applications assigned a specific priority value.

- ◆ Service time is shared at the egress ports by defining scheduling weights for WRR, or for the queuing mode that uses a combination of strict and weighted queuing. Service time is allocated to each queue by calculating a precise number of bytes per second that will be serviced on each round.
- ◆ The specified queue mode applies to all interfaces.

Example

The following example sets the queue mode to strict priority service mode:

```
Console(config)#queue mode strict
Console(config)#
```

Related Commands

[queue weight \(529\)](#)

[show queue mode \(531\)](#)

queue weight This command assigns weights to the eight class of service (CoS) priority queues when using weighted queuing, or one of the queuing modes that use a combination of strict and weighted queuing. Use the **no** form to restore the default weights.

Syntax

queue weight *weight0...weight7*

no queue weight

weight0...weight7 - The ratio of weights for queues 0 - 7 determines the weights used by the WRR scheduler. (Range: 1-15)

Default Setting

Weights 1, 2, 4, 6, 8, 10, 12, 14 are assigned to queues 0 - 7 respectively.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ This command shares bandwidth at the egress port by defining scheduling weights for WRR, or for the queuing mode that uses a combination of strict and weighted queuing ([page 528](#)).
- ◆ Bandwidth is allocated to each queue by calculating a precise number of bytes per second that will be serviced on each round.

Example

The following example shows how to assign round-robin weights of 1 - 4 to the CoS priority queues 0 - 7.

```
Console(config)#queue weight 1 2 3 4 5 6 7 8
Console(config)#
```

Related Commands

[queue mode \(528\)](#)

[show queue weight \(531\)](#)

switchport priority default This command sets a priority for incoming untagged frames. Use the **no** form to restore the default value.

Syntax

switchport priority default *default-priority-id*

no switchport priority default

default-priority-id - The priority number for untagged ingress traffic. The priority is a number from 0 to 7. Seven is the highest priority.

Default Setting

The priority is not set, and the default value for untagged frames received on the interface is zero.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ The precedence for priority mapping is IP DSCP, and then default switchport priority.
- ◆ The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.
- ◆ The switch provides eight priority queues for each port. It can be configured to use strict priority queuing, Weighted Round Robin (WRR), or a combination of strict and weighted queuing using the [queue mode](#) command. Inbound frames that do not have VLAN tags are tagged with the input port's default ingress user priority, and then placed in the appropriate priority queue at the output port. The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in queue 2 of the output port. (Note that if the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.)

Example

The following example shows how to set a default priority on port 3 to 5:

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport priority default 5
Console(config-if)#
```

Related Commands

[show interfaces switchport \(394\)](#)

show queue mode This command shows the current queue mode.

Command Mode

Privileged Exec

Example

```
Console#show queue mode
Unit   Port   queue mode
-----
1      1      Weighted Round Robin
:
```

show queue weight This command displays the weights used for the weighted queues.

Command Mode

Privileged Exec

Example

```
Console#show queue weight
Information of Eth 1/1
Queue ID  Weight
-----
0         1
1         2
2         4
3         6
4         8
5        10
6        12
7        14
:
```

Priority Commands (Layer 3 and 4)

This section describes commands used to configure Layer 3 and 4 traffic priority mapping on the switch.

Table 107: Priority Commands (Layer 3 and 4)

Command	Function	Mode
<code>qos map phb-queue</code>	Maps internal per-hop behavior values to hardware queues	GC
<code>qos map cos-dscp</code>	Maps CoS/CFI values in incoming packets to per-hop behavior and drop precedence values for internal priority processing	IC
<code>qos map default-drop-precedence</code>	Maps the per-hop behavior to default drop precedence	IC
<code>qos map dscp-cos</code>	Maps internal per-hop behavior and drop precedence value pairs to CoS values used in tagged egress packets on a Layer 2 interface	IC
<code>qos map dscp-mutation</code>	Maps DSCP values in incoming packets to per-hop behavior and drop precedence values for internal priority processing	IC
<code>qos map ip-port-dscp</code>	Maps the destination TCP/UDP port in incoming packets to per-hop behavior and drop precedence values for internal priority processing	IC
<code>qos map ip-prec-dscp</code>	Maps IP Precedence values in incoming packets to per-hop behavior and drop precedence values for internal priority processing	IC
<code>qos map trust-mode</code>	Sets QoS mapping to DSCP or CoS	IC
<code>show qos map cos-dscp</code>	Shows ingress CoS to internal DSCP map	PE
<code>show map default-drop-precedence</code>	Shows the per-hop behavior to default drop precedence	PE
<code>show map dscp-cos</code>	Shows internal DSCP to egress CoS map	PE
<code>show qos map dscp-mutation</code>	Shows ingress DSCP to internal DSCP map	PE
<code>show qos map ip-port-dscp</code>	Shows destination TCP/UDP port to internal DSCP map	PE
<code>show qos map ip-prec-dscp</code>	Shows ingress IP Precedence to internal DSCP map	PE
<code>show qos map phb-queue</code>	Shows internal per-hop behavior to hardware queue map	PE
<code>show qos map trust-mode</code>	Shows the QoS mapping mode	PE

* The default settings used for mapping priority values to internal DSCP values and back to the hardware queues are designed to optimize priority services for the majority of network applications. It should not be necessary to modify any of the default settings unless a queuing problem occurs with a particular application.

qos map phb-queue This command determines the hardware output queues to use based on the internal per-hop behavior value. Use the **no** form to restore the default settings.

Syntax

qos map phb-queue *queue-id* **from** *phb0 ... phb7*

no map phb-queue *phb0 ... phb7*

phb - Per-hop behavior, or the priority used for this router hop. (Range: 0-7)

queue-id - The ID of the priority queue. (Range: 0-7, where 7 is the highest priority queue)

DEFAULT SETTING.

Table 108: Mapping Internal Per-hop Behavior to Hardware Queues

Per-hop Behavior	0	1	2	3	4	5	6	7
Hardware Queues	2	0	1	3	4	5	6	7

Command Mode

Global Configuration

Command Usage

- ◆ Enter a queue identifier, followed by the keyword “from” and then up to eight internal per-hop behavior values separated by spaces.
- ◆ Egress packets are placed into the hardware queues according to the mapping defined by this command.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#qos map phb-queue 0 from 1 2 3
Console(config-if)#
```

qos map cos-dscp This command maps CoS/CFI values in incoming packets to per-hop behavior and drop precedence values for priority processing. Use the **no** form to restore the default settings.

Syntax

qos map cos-dscp *phb drop-precedence* **from** *cos0 cfi0...cos7 cfi7*

no qos map cos-dscp *cos0 cfi0...cos7 cfi7*

phb - Per-hop behavior, or the priority used for this router hop. (Range: 0-7)

drop-precedence - Drop precedence used for controlling traffic congestion.
(Range: 0 - Green, 3 - Yellow, 1 - Red)

cos - CoS value in ingress packets. (Range: 0-7)

cfi - Canonical Format Indicator. Set to this parameter to "0" to indicate that the MAC address information carried in the frame is in canonical format.
(Range: 0-1)

DEFAULT SETTING.

Table 109: Default Mapping of CoS/CFI to Internal PHB/Drop Precedence

CoS	CFI	0	1
0		(0,0)	(0,0)
1		(1,0)	(1,0)
2		(2,0)	(2,0)
3		(3,0)	(3,0)
4		(4,0)	(4,0)
5		(5,0)	(5,0)
6		(6,0)	(6,0)
7		(7,0)	(7,0)

Command Mode

Interface Configuration (Port, Static Aggregation)

Command Usage

- ◆ The default mapping of CoS to PHB values shown in [Table 109](#) is based on the recommended settings in IEEE 802.1p for mapping CoS values to output queues.
- ◆ Enter a value pair for the internal per-hop behavior and drop precedence, followed by the keyword "from" and then up to eight CoS/CFI paired values separated by spaces.
- ◆ If a packet arrives with a 802.1Q header but it is not an IP packet, then the CoS/CFI-to-PHB/Drop Precedence mapping table is used to generate priority and

drop precedence values for internal processing. Note that priority tags in the original packet are not modified by this command.

- ◆ The specified mapping applies to all interfaces.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#qos map cos-dscp 0 0 from 0 1
Console(config-if)#
```

qos map default-drop-precedence

This command maps the internal per-hop behavior (based on packet priority) to a default drop precedence for internal processing of untagged packets. Use the **no** form to restore the default settings.

Syntax

qos map default-drop-precedence *drop-precedence* **from** *phb0 ... phb7*

no map default-drop-precedence *phb0 ... phb7*

drop-precedence - Drop precedence used for controlling traffic congestion.
(Range: 0 - Green, 3 - Yellow, 1 - Red)

phb - Per-hop behavior, or the priority used for this router hop. (Range: 0-7)

DEFAULT SETTING.

Table 110: Mapping Per-hop Behavior to Drop Precedence

Per-hop Behavior	0	1	2	3	4	5	6	7
Drop Precedence	0	0	0	0	0	0	0	0

Command Mode

Interface Configuration (Port, Static Aggregation)

Command Usage

- ◆ Enter a drop precedence, followed by the keyword “from” and then up to four per-hop behavior values separated by spaces.
- ◆ This command only applies to Layer 2 untagged ingress packets. The drop precedence for any priority tagged ingress packets will be based on the other corresponding QoS mapping schemes described in those sections.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#qos map default-drop-precedence 1 from 0 1 2
Console(config-if)#qos map default-drop-precedence 3 from 3 4 5
Console(config-if)#qos map default-drop-precedence 0 from 6 7
Console(config-if)#
```

qos map dscp-cos This command maps internal per-hop behavior and drop precedence value pairs to CoS/CFI values used in tagged egress packets on a Layer 2 interface. Use the **no** form to restore the default settings.

Syntax

qos map dscp-cos *cos-value cfi-value from phb0 drop-precedence0 ... phb7 drop-precedence7*

no map ip dscp *phb0 drop-precedence0 ... phb7 drop-precedence7*
cos-value - CoS value in ingress packets. (Range: 0-7)

cfi-value - Canonical Format Indicator. Set to this parameter to "0" to indicate that the MAC address information carried in the frame is in canonical format. (Range: 0-1)

phb - Per-hop behavior, or the priority used for this router hop. (Range: 0-7)

drop-precedence - Drop precedence used for controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)

DEFAULT SETTING

Table 111: Mapping Internal PHB/Drop Precedence to CoS/CFI Values

Drop Precedence	0 (green)	1 (red)	3 (yellow)
Per-hop Behavior			
0	(0,0)	(0,0)	(0,0)
1	(1,0)	(1,0)	(1,0)
2	(2,0)	(2,0)	(2,0)
3	(3,0)	(3,0)	(3,0)
4	(4,0)	(4,0)	(4,0)
5	(5,0)	(5,0)	(5,0)
6	(6,0)	(6,0)	(6,0)
7	(7,0)	(7,0)	(7,0)

Command Mode

Interface Configuration (Port, Static Aggregation)

Command Usage

- ◆ Enter a CoS/CFI value pair, followed by the keyword "from" and then four internal per-hop behavior and drop precedence value pairs separated by spaces.
- ◆ If the packet is forwarded with an 8021.Q tag, the priority value in the egress packet is modified based on the table shown above, or on similar values as modified by this command.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#qos map dscp-cos 1 0 from 1 2
Console(config-if)#
```

qos map dscp-mutation This command maps DSCP values in incoming packets to per-hop behavior and drop precedence values for priority processing. Use the **no** form to restore the default settings.

Syntax

qos map dscp-mutation *phb drop-precedence* **from** *dscp0 ... dscp7*

no qos map dscp-mutation *dscp0 ... dscp7*

phb - Per-hop behavior, or the priority used for this router hop. (Range: 0-7)

drop-precedence - Drop precedence used for in controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)

dscp - DSCP value in ingress packets. (Range: 0-63)

DEFAULT SETTING.

Table 112: Default Mapping of DSCP Values to Internal PHB/Drop Values

	ingress-dscp1	0	1	2	3	4	5	6	7	8	9
ingress-dscp10											
0		0,0	0,1	0,0	0,3	0,0	0,1	0,0	0,3	1,0	1,1
1		1,0	1,3	1,0	1,1	1,0	1,3	2,0	2,1	2,0	2,3
2		2,0	2,1	2,0	2,3	3,0	3,1	3,0	3,3	3,0	3,1
3		3,0	3,3	4,0	4,1	4,0	4,3	4,0	4,1	4,0	4,3
4		5,0	5,1	5,0	5,3	5,0	5,1	6,0	5,3	6,0	6,1
5		6,0	6,3	6,0	6,1	6,0	6,3	7,0	7,1	7,0	7,3
6		7,0	7,1	7,0	7,3						

The ingress DSCP is composed of ingress-dscp10 (most significant digit in the left column) and ingress-dscp1 (least significant digit in the top row (in other words, ingress-dscp = ingress-dscp10 * 10 + ingress-dscp1); and the corresponding internal-dscp is shown at the intersecting cell in the table.

The ingress DSCP is bitwise ANDed with the binary value 11 to determine the drop precedence. If the resulting value is 10 binary, then the drop precedence is set to 0.

Command Mode

Interface Configuration (Port, Static Aggregation)

Command Usage

- ◆ Enter a value pair for the internal per-hop behavior and drop precedence, followed by the keyword “from” and then up to eight DSCP values separated by spaces.
- ◆ This map is only used when the QoS mapping mode is set to “DSCP” by the `qos map trust-mode` command, and the ingress packet type is IPv4.
- ◆ Two QoS domains can have different DSCP definitions, so the DSCP-to-PHB/ Drop Precedence mutation map can be used to modify one set of DSCP values to match the definition of another domain. The mutation map should be applied at the receiving port (ingress mutation) at the boundary of a QoS administrative domain.
- ◆ The specified mapping applies to all interfaces.

Example

This example changes the priority for all packets entering port 1 which contain a DSCP value of 1 to a per-hop behavior of 3 and a drop precedence of 1. Referring to [Table 112](#), note that the DSCP value for these packets is now set to 25 ($3 \times 2^3 + 1$) and passed on to the egress interface.

```
Console(config)#interface ethernet 1/5
Console(config-if)#qos map dscp-mutation 3 1 from 1
Console(config-if)#
```

qos map ip-port-dscp This command maps the destination TCP/UDP destination port in incoming packets to per-hop behavior and drop precedence values for priority processing. Use the **no** form to remove the mapped values for a TCP/UDP port.

Syntax

qos map ip-port-dscp {tcp | udp} port-number to phb drop-precedence

no qos map ip-port-dscp {tcp | udp} port-number

phb - Per-hop behavior, or the priority used for this router hop. (Range: 0-7)

drop-precedence - Drop precedence used for controlling traffic congestion.
(Range: 0 - Green, 3 - Yellow, 1 - Red)

tcp - Transport Control Protocol

udp - User Datagram Protocol

port-number - 16-bit TCP/UDP destination port number. (Range: 0-65535)

Default Setting

None

Command Mode

Interface Configuration (Port, Static Aggregation)

Command Usage

- ◆ This mapping table is only used if the protocol type of the arriving packet is TCP or UDP.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#qos map ip-port-dscp tcp 21 to 1 0
Console(config-if)#
```

qos map ip-prec-dscp This command maps IP precedence values in incoming packets to per-hop behavior and drop precedence values for priority processing. Use the **no** form to restore the default settings.

Syntax

qos map ip-prec-dscp *phb0 drop-precedence0 ... phb7 drop-precedence7*

no map ip-prec-dscp

phb - Per-hop behavior, or the priority used for this router hop. (Range: 0-7)

drop-precedence - Drop precedence used for controlling traffic congestion.
(Range: 0 - Green, 3 - Yellow, 1 - Red)

DEFAULT SETTING.

Table 113: Default Mapping of IP Precedence to Internal PHB/Drop Values

IP Precedence Value	0	1	2	3	4	5	6	7
Per-hop Behavior	0	1	2	3	4	5	6	7
Drop Precedence	0	0	0	0	0	0	0	0

Command Mode

Interface Configuration (Port, Static Aggregation)

Command Usage

- ◆ Enter up to eight paired values for per-hop behavior and drop precedence separated by spaces. These values are used for internal priority processing, and correspond to IP Precedence values 0 - 7.
- ◆ If the QoS mapping mode is set the IP Precedence and the ingress packet type is IPv4, then the IP Precedence-to-DSCP mapping table is used to generate priority and drop precedence values for internal processing.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#qos map ip-prec-dscp 7 0 6 0 5 0 4 0 3 0 2 1 1 1 0 1
Console(config-if)#
```

qos map trust-mode This command sets QoS mapping to DSCP or CoS. Use the **no** form to restore the default setting.

Syntax

qos map trust-mode {cos | dscp | ip-prec}

no qos map trust-mode

cos - Sets the QoS mapping mode to CoS.

dscp - Sets the QoS mapping mode to DSCP.

ip-prec - Sets the QoS mapping mode to IP Precedence.

Default Setting

CoS

Command Mode

Interface Configuration (Port, Static Aggregation)

Command Usage

- ◆ If the QoS mapping mode is set to IP Precedence with this command, and the ingress packet type is IPv4, then priority processing will be based on the IP Precedence value in the ingress packet.
- ◆ If the QoS mapping mode is set to DSCP with this command, and the ingress packet type is IPv4, then priority processing will be based on the DSCP value in the ingress packet.
- ◆ If the QoS mapping mode is set to either IP Precedence or DSCP, and a non-IP packet is received, the packet's CoS and CFI (Canonical Format Indicator) values are used for priority processing if the packet is tagged. For an untagged packet, the default port priority (see [page 530](#)) is used for priority processing.
- ◆ If the QoS mapping mode is set to CoS with this command, and the ingress packet type is IPv4, then priority processing will be based on the CoS and CFI values in the ingress packet.

For an untagged packet, the default port priority (see [page 530](#)) is used for priority processing.

Example

This example sets the QoS priority mapping mode to use DSCP based on the conditions described in the Command Usage section.

```
Console(config)#interface ge1/1
Console(config-if)#qos map trust-mode dscp
Console(config-if)#
```

show qos map cos-dscp This command shows ingress CoS/CFI to internal DSCP map.

Syntax

show qos map cos-dscp interface *interface*

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Command Mode

Privileged Exec

Example

```
Console#show qos map cos-dscp interface ethernet 1/5
CoS Information of Eth 1/5
CoS-DSCP map. (x,y),x: phb,y: drop precedence:
CoS   : CFI   0           1
-----
0           (0,0)        (0,0)
1           (1,0)        (1,0)
2           (2,0)        (2,0)
3           (3,0)        (3,0)
4           (4,0)        (4,0)
5           (5,0)        (5,0)
6           (6,0)        (6,0)
7           (7,0)        (7,0)
Console#
```

show map default-drop-precedence This command shows the per-hop behavior to default drop precedence for untagged ingress packets.

Syntax

show qos map default-drop-precedence interface *interface*

ethernet *unit/port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Command Mode

Privileged Exec

Example

```
Console#show qos map default-drop-precedence interface ethernet 1/5
Information of Eth 1/5
default-drop-precedence map:
phb:      0      1      2      3      4      5      6      7
-----
color:    0      0      0      0      0      0      0      0
Console#
```

show map dscp-cos This command shows the internal DSCP to egress CoS map, which converts internal PHB/Drop Precedence to CoS values.

Syntax

```
show qos map dscp-cos interface interface
                                interface
                                ethernet unit/port
                                    unit - Stack unit. (Range: 1)
                                    port - Port number. (Range: 1-52)
                                port-channel channel-id (Range: 1-8)
```

Command Mode

Privileged Exec

Command Usage

This map is only used if the packet is forwarded with a 8021.Q tag.

Example

```
Console#show qos map dscp-cos interface ethernet 1/5
Information of Eth 1/5
dscp-cos map:
phb:  drop precedence    0 (green)    1 (red)    3 (yellow)
-----
0  :                      (0,0)      (0,0)      (0,0)
1  :                      (1,0)      (1,0)      (1,0)
2  :                      (2,0)      (2,0)      (2,0)
3  :                      (3,0)      (3,0)      (3,0)
4  :                      (4,0)      (4,0)      (4,0)
5  :                      (5,0)      (5,0)      (5,0)
6  :                      (6,0)      (6,0)      (6,0)
7  :                      (7,0)      (7,0)      (7,0)
Console#
```

show qos map dscp-mutation This command shows the ingress DSCP to internal DSCP map.

Syntax

show qos map dscp-mutation interface *interface*
interface
ethernet *unit/port*
unit - Unit identifier. (Range: 1)
port - Port number. (Range: 1-52)
port-channel *channel-id* (Range: 1-8)

Command Mode

Privileged Exec

Command Usage

This map is only used when the QoS mapping mode is set to "DSCP" by the [qos map trust-mode](#) command, and the ingress packet type is IPv4.

Example

The ingress DSCP is composed of "d1" (most significant digit in the left column) and "d2" (least significant digit in the top row (in other words, ingress DSCP = d1 * 10 + d2); and the corresponding Internal DSCP and drop precedence is shown at the intersecting cell in the table.

```
Console#show qos map dscp-mutation interface ethernet 1/5
DSCP mutation map.(x,y),x: PHB,y: drop precedence:
d1: d2 0    1    2    3    4    5    6    7    8    9
-----
0 :   (0,0) (0,1) (0,0) (0,3) (0,0) (0,1) (0,0) (0,3) (1,0) (1,1)
1 :   (1,0) (1,3) (1,0) (1,1) (1,0) (1,3) (2,0) (2,1) (2,0) (2,3)
2 :   (2,0) (2,1) (2,0) (2,3) (3,0) (3,1) (3,0) (3,3) (3,0) (3,1)
3 :   (3,0) (3,3) (4,0) (4,1) (4,0) (4,3) (4,0) (4,1) (4,0) (4,3)
4 :   (5,0) (5,1) (5,0) (5,3) (5,0) (5,1) (6,0) (5,3) (6,0) (6,1)
5 :   (6,0) (6,3) (6,0) (6,1) (6,0) (6,3) (7,0) (7,1) (7,0) (7,3)
6 :   (7,0) (7,1) (7,0) (7,3)
```

show qos map ip-port-dscp This command shows the ingress TCP/UDP port to internal DSCP map.

Syntax

show qos map ip-port-dscp interface *interface*
interface
ethernet *unit/port*
unit - Stack unit. (Range: 1)
port - Port number. (Range: 1-52)
port-channel *channel-id* (Range: 1-8)

Command Mode

Privileged Exec

Command Usage

The IP Port-to-DSCP mapping table is only used if the protocol type of the arriving packet is TCP or UDP.

Example

```
Console#show qos map ip-port-dscp interface ethernet 1/5
Information of Eth 1/5
ip-port-dscp map:
(ip protocol,destination port) :   phb       drop precedence
-----
(TCP, 21)      :                0         0
(UDP, 12)      :                1         0
Console#
```

show qos map ip-prec-dscp This command shows the ingress IP precedence to internal DSCP map.

Syntax

show qos map ip-prec-dscp interface *interface*

ethernet *unit/port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Command Mode

Privileged Exec

Command Usage

If the QoS mapping mode is set to IP Precedence and the ingress packet type is IPv4, then the IP Precedence-to-DSCP mapping table is used to generate per-hop behavior and drop precedence values for internal processing.

Example

```
Console#show qos map ip-prec-dscp interface ethernet 1/5
Information of Eth 1/5
IP-prec-DSCP map:
IP-prec:      0      1      2      3      4      5      6      7
-----
PHB:          0      1      2      3      4      5      6      7
drop precedence: 0      0      0      0      0      0      0      0
Console#
```


show qos map phb-queue This command shows internal per-hop behavior to hardware queue map.

Syntax

show qos map phb-queue interface *interface*
interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Command Mode

Privileged Exec

Example

```
Console#show qos map phb-queue interface ethernet 1/5
Information of Eth 1/5
PHB-queue map:
PHB:      0      1      2      3      4      5      6      7
-----
queue:    2      0      1      3      4      5      6      7
Console#
```

show qos map trust-mode This command shows the QoS mapping mode.

Syntax

show qos map trust-mode interface *interface*
interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Command Mode

Privileged Exec

Example

The following shows that the trust mode is set to CoS:

```
Console#show qos map trust-mode interface ethernet 1/5
Information of Eth 1/5
CoS Map Mode:          CoS mode
Console#
```


Quality of Service Commands

The commands described in this section are used to configure Differentiated Services (DiffServ) classification criteria and service policies. You can classify traffic based on access lists, IP Precedence or DSCP values, or VLANs. Using access lists allows you select traffic based on Layer 2, Layer 3, or Layer 4 information contained in each packet.

Table 114: Quality of Service Commands

Command	Function	Mode
class-map	Creates a class map for a type of traffic	GC
description	Specifies the description of a class map	CM
match	Defines the criteria used to classify traffic	CM
rename	Redefines the name of a class map	CM
policy-map	Creates a policy map for multiple interfaces	GC
description	Specifies the description of a policy map	PM
class	Defines a traffic classification for the policy to act on	PM
rename	Redefines the name of a policy map	PM
police flow	Defines an enforcer for classified traffic based on a metered flow rate	PM-C
police srtcm-color	Defines an enforcer for classified traffic based on a single rate three color meter	PM-C
police trtcm-color	Defines an enforcer for classified traffic based on a two rate three color meter	PM-C
set cos	Serves IP traffic by setting a class of service value for matching packets for internal processing	PM-C
set phb	Serves IP traffic by setting a per-hop behavior value for matching packets for internal processing	PM-C
service-policy	Applies a policy map defined by the policy-map command to the input of a particular interface	IC
show class-map	Displays the QoS class maps which define matching criteria used for classifying traffic	PE
show policy-map	Displays the QoS policy maps which define classification criteria for incoming traffic, and may include policers for bandwidth limitations	PE
show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface	PE

To create a service policy for a specific category of ingress traffic, follow these steps:

1. Use the **class-map** command to designate a class name for a specific category of traffic, and enter the Class Map configuration mode.
2. Use the **match** command to select a specific type of traffic based on an access list, an IPv4 DSCP value, IPv4 Precedence value, a VLAN, or a CoS value.
3. Use the **policy-map** command to designate a policy name for a specific manner in which ingress traffic will be handled, and enter the Policy Map configuration mode.
4. Use the **class** command to identify the class map, and enter Policy Map Class configuration mode. A policy map can contain up to 16 class maps.
5. Use the **set phb** or **set cos** command to modify the per-hop behavior, the class of service value in the VLAN tag for the matching traffic class, and use one of the **police** commands to monitor parameters such as the average flow and burst rate, and drop any traffic that exceeds the specified rate, or just reduce the DSCP service level for traffic exceeding the specified rate.
6. Use the **service-policy** command to assign a policy map to a specific interface.



Note: Create a Class Map before creating a Policy Map.

class-map This command creates a class map used for matching packets to the specified class, and enters Class Map configuration mode. Use the **no** form to delete a class map.

Syntax

[no] class-map *class-map-name* **match-any**

class-map-name - Name of the class map. (Range: 1-32 characters)

match-any - Match any condition within a class map.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ First enter this command to designate a class map and enter the Class Map configuration mode. Then use **match** commands to specify the criteria for ingress traffic that will be classified under this class map.

- ◆ One or more class maps can be assigned to a policy map ([page 551](#)). The policy map is then bound by a service policy to an interface ([page 561](#)). A service policy defines packet classification, service tagging, and bandwidth policing. Once a policy map has been bound to an interface, no additional class maps may be added to the policy map, nor any changes made to the assigned class maps with the **match** or **set** commands.

Example

This example creates a class map call “rd-class,” and sets it to match packets marked for DSCP service value 3:

```
Console(config)#class-map rd-class match-any
Console(config-cmap)#match ip dscp 3
Console(config-cmap)#
```

Related Commands

[show class-map \(561\)](#)

description This command specifies the description of a class map or policy map.

Syntax

description *string*

string - Description of the class map or policy map. (Range: 1-64 characters)

Command Mode

Class Map Configuration

Policy Map Configuration

Example

```
Console(config)#class-map rd-class#1
Console(config-cmap)#description matches packets marked for DSCP service
value 3
Console(config-cmap)#
```

match This command defines the criteria used to classify traffic. Use the **no** form to delete the matching criteria.

Syntax

[no] match {**access-list** *acl-name* | **cos** *cos* | **ip dscp** *dscp* |
ip precedence *ip-precedence* | **source-port** *interface* | **vlan** *vlan*}

acl-name - Name of the access control list. Any type of ACL can be specified, including standard or extended IP ACLs and MAC ACLs.
(Range: 1-16 characters)

cos - A Class of Service value. (Range: 0-7)

dscp - A Differentiated Service Code Point value. (Range: 0-63)

ip-precedence - An IP Precedence value. (Range: 0-7)

vlan - A VLAN. (Range:1-4094)

Default Setting

None

Command Mode

Class Map Configuration

Command Usage

- ◆ First enter the **class-map** command to designate a class map and enter the Class Map configuration mode. Then use **match** commands to specify the fields within ingress packets that must match to qualify for this class map.
- ◆ If an ingress packet matches an ACL specified by this command, any deny rules included in the ACL will be ignored.
- ◆ If match criteria includes an IP ACL or IP priority rule, then a VLAN rule cannot be included in the same class map.
- ◆ If match criteria includes a MAC ACL or VLAN rule, then neither an IP ACL nor IP priority rule can be included in the same class map.
- ◆ Up to 16 match entries can be included in a class map.

Example

This example creates a class map called "rd-class#1," and sets it to match packets marked for DSCP service value 3.

```
Console(config)#class-map rd-class#1 match-any
Console(config-cmap)#match ip dscp 3
Console(config-cmap)#
```

This example creates a class map call "rd-class#2," and sets it to match packets marked for IP Precedence service value 5.

```
Console(config)#class-map rd-class#2 match-any
Console(config-cmap)#match ip precedence 5
Console(config-cmap)#
```

This example creates a class map call “rd-class#3,” and sets it to match packets marked for VLAN 1.

```
Console(config)#class-map rd-class#3 match-any
Console(config-cmap)#match vlan 1
Console(config-cmap)#
```

rename This command redefines the name of a class map or policy map.

Syntax

rename *map-name*

map-name - Name of the class map or policy map. (Range: 1-32 characters)

Command Mode

Class Map Configuration

Policy Map Configuration

Example

```
Console(config)#class-map rd-class#1
Console(config-cmap)#rename rd-class#9
Console(config-cmap)#
```

policy-map This command creates a policy map that can be attached to multiple interfaces, and enters Policy Map configuration mode. Use the **no** form to delete a policy map.

Syntax

[no] policy-map *policy-map-name*

policy-map-name - Name of the policy map. (Range: 1-32 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ Use the **policy-map** command to specify the name of the policy map, and then use the **class** command to configure policies for traffic that matches the criteria defined in a class map.
- ◆ A policy map can contain multiple class statements that can be applied to the same interface with the **service-policy** command.

- ◆ Create a Class Map ([page 551](#)) before assigning it to a Policy Map.

Example

This example creates a policy called “rd-policy,” uses the [class](#) command to specify the previously defined “rd-class,” uses the **set** command to classify the service that incoming packets will receive, and then uses the [police flow](#) command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4000 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set cos 0
Console(config-pmap-c)#police flow 10000 4000 conform-action transmit
violate-action drop
Console(config-pmap-c)#
```

class This command defines a traffic classification upon which a policy can act, and enters Policy Map Class configuration mode. Use the **no** form to delete a class map.

Syntax

[no] class *class-map-name*

class-map-name - Name of the class map. (Range: 1-32 characters)

Default Setting

None

Command Mode

Policy Map Configuration

Command Usage

- ◆ Use the [policy-map](#) command to specify a policy map and enter Policy Map configuration mode. Then use the **class** command to enter Policy Map Class configuration mode. And finally, use the **set** command and one of the **police** commands to specify the match criteria, where the:
 - [set phb](#) command sets the per-hop behavior value in matching packets. (This modifies packet priority for internal processing only.)
 - [set cos](#) command sets the class of service value in matching packets. (This modifies packet priority in the VLAN tag.)
 - **police** commands define parameters such as the maximum throughput, burst rate, and response to non-conforming traffic.
- ◆ Up to 16 classes can be included in a policy map.

Example

This example creates a policy called “rd-policy,” uses the **class** command to specify the previously defined “rd-class,” uses the **set phb** command to classify the service that incoming packets will receive, and then uses the **police flow** command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4,000 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set phb 3
Console(config-pmap-c)#police flow 10000 4000 conform-action transmit
violate-action drop
Console(config-pmap-c)#
```

police flow This command defines an enforcer for classified traffic based on the metered flow rate. Use the **no** form to remove a policer.

Syntax

[no] police flow *committed-rate committed-burst*
conform-action {**transmit** | *new-dscp*}
violate-action {**drop** | *new-dscp*}

committed-rate - Committed information rate (CIR) in kilobits per second.
 (Range: 0-1000000 kbps or maximum port speed, whichever is lower)

committed-burst - Committed burst size (BC) in bytes.
 (Range: 0-524288 bytes)

conform-action - Action to take when packet is within the CIR and BC.
 (There are enough tokens to service the packet, the packet is set green).

violate-action - Action to take when packet exceeds the CIR and BC. (There are not enough tokens to service the packet, the packet is set red).

transmit - Transmits without taking any action.

drop - Drops packet as required by violate-action.

new-dscp - Differentiated Service Code Point (DSCP) value. (Range: 0-63)

Default Setting

None

Command Mode

Policy Map Class Configuration

Command Usage

- ◆ You can configure up to 16 policers (i.e., class maps) for ingress ports.
- ◆ Policing is based on a token bucket, where bucket depth (i.e., the maximum burst before the bucket overflows) is by specified the *committed-burst* field, and the average rate tokens are added to the bucket is by specified by the

committed-rate option. Note that the token bucket functions similar to that described in RFC 2697 and RFC 2698.

- ◆ The behavior of the meter is specified in terms of one token bucket (C), the rate at which the tokens are incremented (CIR – Committed Information Rate), and the maximum size of the token bucket (BC – Committed Burst Size).

The token bucket C is initially full, that is, the token count $T_c(0) = BC$. Thereafter, the token count T_c is updated CIR times per second as follows:

- If T_c is less than BC, T_c is incremented by one, else
- T_c is not incremented.

When a packet of size B bytes arrives at time t, the following happens:

- If $T_c(t) - B \geq 0$, the packet is green and T_c is decremented by B down to the minimum value of 0, else
- else the packet is red and T_c is not decremented.

Example

This example creates a policy called “rd-policy,” uses the **class** command to specify the previously defined “rd-class,” uses the **set phb** command to classify the service that incoming packets will receive, and then uses the **police flow** command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4000 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set phb 3
Console(config-pmap-c)#police flow 100000 4000 conform-action transmit
violate-action drop
Console(config-pmap-c)#
```

police srtcm-color This command defines an enforcer for classified traffic based on a single rate three color meter (srTCM). Use the **no** form to remove a policer.

Syntax

```
[no] police {srtcm-color-blind | srtcm-color-aware}
    committed-rate committed-burst excess-burst
    conform-action {transmit | new-dscp}
    exceed-action {drop | new-dscp}
    violate action {drop | new-dscp}
```

srtcm-color-blind - Single rate three color meter in color-blind mode.

srtcm-color-aware - Single rate three color meter in color-aware mode.

committed-rate - Committed information rate (CIR) in kilobits per second.
(Range: 0-1000000 kbps or maximum port speed, whichever is lower)

committed-burst - Committed burst size (BC) in bytes.
(Range: 0-524288 bytes)

excess-burst - Excess burst size (BE) in bytes. (Range: 0-524288 bytes)

conform-action - Action to take when rate is within the CIR and BC. (There are enough tokens in bucket BC to service the packet, packet is set green).

exceed-action - Action to take when rate exceeds the CIR and BC but is within the BE. (There are enough tokens in bucket BE to service the packet, the packet is set yellow.)

violate-action - Action to take when rate exceeds the BE. (There are not enough tokens in bucket BE to service the packet, the packet is set red.)

transmit - Transmits without taking any action.

drop - Drops packet as required by exceed-action or violate-action.

new-dscp - Differentiated Service Code Point (DSCP) value. (Range: 0-63)

Default Setting

None

Command Mode

Policy Map Class Configuration

Command Usage

- ◆ You can configure up to 16 policers (i.e., class maps) for ingress ports.
- ◆ The srTCM as defined in RFC 2697 meters a traffic stream and processes its packets according to three traffic parameters – Committed Information Rate (CIR), Committed Burst Size (BC), and Excess Burst Size (BE).
- ◆ The PHB label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion. A packet is marked green if it doesn't exceed the CIR and BC, yellow if it does exceed the CIR and BC, but not the BE, and red otherwise.
- ◆ The meter operates in one of two modes. In the color-blind mode, the meter assumes that the packet stream is uncolored. In color-aware mode the meter assumes that some preceding entity has pre-colored the incoming packet stream so that each packet is either green, yellow, or red. The meter (re)colors an IP packet according to the results of the meter. The color is coded in the DS field [RFC 2474] of the packet.
- ◆ The behavior of the meter is specified in terms of its mode and two token buckets, C and E, which both share the common rate CIR. The maximum size of the token bucket C is BC and the maximum size of the token bucket E is BE.

The token buckets C and E are initially full, that is, the token count $Tc(0) = BC$ and the token count $Te(0) = BE$. Thereafter, the token counts Tc and Te are updated CIR times per second as follows:

- If Tc is less than BC, Tc is incremented by one, else
- if Te is less than BE, Te is incremented by one, else
- neither Tc nor Te is incremented.

When a packet of size B bytes arrives at time t, the following happens if srTCM is configured to operate in color-blind mode:

- If $Tc(t) - B \geq 0$, the packet is green and Tc is decremented by B down to the minimum value of 0, else
- if $Te(t) - B \geq 0$, the packet is yellow and Te is decremented by B down to the minimum value of 0,
- else the packet is red and neither Tc nor Te is decremented.

When a packet of size B bytes arrives at time t, the following happens if srTCM is configured to operate in color-aware mode:

- If the packet has been precolored as green and $Tc(t) - B \geq 0$, the packet is green and Tc is decremented by B down to the minimum value of 0, else
- If the packet has been precolored as yellow or green and if
- $Te(t) - B \geq 0$, the packet is yellow and Te is decremented by B down to the minimum value of 0, else the packet is red and neither Tc nor Te is decremented.

The metering policy guarantees a deterministic behavior where the volume of green packets is never smaller than what has been determined by the CIR and BC, that is, tokens of a given color are always spent on packets of that color. Refer to RFC 2697 for more information on other aspects of srTCM.

Example

This example creates a policy called "rd-policy," uses the `class` command to specify the previously defined "rd-class," uses the `set phb` command to classify the service that incoming packets will receive, and then uses the **`police srtcm-color-blind`** command to limit the average bandwidth to 100,000 Kbps, the committed burst rate to 4000 bytes, the excess burst rate to 6000 bytes, to remark any packets exceeding the committed burst size, and to drop any packets exceeding the excess burst size.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set phb 3
Console(config-pmap-c)#police srtcm-color-blind 100000 4000 6000 conform-
  action transmit exceed-action 0 violate-action drop
Console(config-pmap-c)#
```

police trtcm-color This command defines an enforcer for classified traffic based on a two rate three color meter (trTCM). Use the **no** form to remove a policer.

Syntax

```
[no] police {trtcm-color-blind | trtcm-color-aware}
    committed-rate committed-burst peak-rate peak-burst
    conform-action {transmit | new-dscp}
    exceed-action {drop | new-dscp}
    violate action {drop | new-dscp}
```

trtcm-color-blind - Two rate three color meter in color-blind mode.

trtcm-color-aware - Two rate three color meter in color-aware mode.

committed-rate - Committed information rate (CIR) in kilobits per second.
(Range: 0-1000000 kbps or maximum port speed, whichever is lower)

committed-burst - Committed burst size (BC) in bytes.
(Range: 0-524288 bytes)

peak-rate - Peak information rate (PIR) in kilobits per second.
(Range: 0-1000000 kbps or maximum port speed, whichever is lower)

peak-burst - Peak burst size (BP) in bytes. (Range: 0-524288 bytes)

conform-action - Action to take when rate is within the CIR and BP. (Packet size does not exceed BP and there are enough tokens in bucket BC to service the packet, the packet is set green.)

exceed-action - Action to take when rate exceeds the CIR but is within the PIR. (Packet size exceeds BC but there are enough tokens in bucket BP to service the packet, the packet is set yellow.)

violate-action - Action to take when rate exceeds the PIR. (There are not enough tokens in bucket BP to service the packet, the packet is set red.)

drop - Drops packet as required by exceed-action or violate-action.

transmit - Transmits without taking any action.

new-dscp - Differentiated Service Code Point (DSCP) value. (Range: 0-63)

Default Setting

None

Command Mode

Policy Map Class Configuration

Command Usage

- ◆ You can configure up to 16 policers (i.e., class maps) for ingress ports.
- ◆ The trTCM as defined in RFC 2698 meters a traffic stream and processes its packets based on two rates – Committed Information Rate (CIR) and Peak Information Rate (PIR), and their associated burst sizes - Committed Burst Size (BC) and Peak Burst Size (BP).

- ◆ The PHB label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion. A packet is marked red if it exceeds the PIR. Otherwise it is marked either yellow or green depending on whether it exceeds or doesn't exceed the CIR.

The trTCM is useful for ingress policing of a service, where a peak rate needs to be enforced separately from a committed rate.

- ◆ The meter operates in one of two modes. In the color-blind mode, the meter assumes that the packet stream is uncolored. In color-aware mode the meter assumes that some preceding entity has pre-colored the incoming packet stream so that each packet is either green, yellow, or red. The marker (re)colors an IP packet according to the results of the meter. The color is coded in the DS field [RFC 2474] of the packet.
- ◆ The behavior of the meter is specified in terms of its mode and two token buckets, P and C, which are based on the rates PIR and CIR, respectively. The maximum size of the token bucket P is BP and the maximum size of the token bucket C is BC.
- ◆ The token buckets P and C are initially (at time 0) full, that is, the token count $Tp(0) = BP$ and the token count $Tc(0) = BC$. Thereafter, the token count Tp is incremented by one PIR times per second up to BP and the token count Tc is incremented by one CIR times per second up to BC.

When a packet of size B bytes arrives at time t, the following happens if trTCM is configured to operate in color-blind mode:

- If $Tp(t) - B < 0$, the packet is red, else
- if $Tc(t) - B < 0$, the packet is yellow and Tp is decremented by B, else
- the packet is green and both Tp and Tc are decremented by B.

When a packet of size B bytes arrives at time t, the following happens if trTCM is configured to operate in color-aware mode:

- If the packet has been precolored as red or if $Tp(t) - B < 0$, the packet is red, else
- if the packet has been precolored as yellow or if $Tc(t) - B < 0$, the packet is yellow and Tp is decremented by B, else
- the packet is green and both Tp and Tc are decremented by B.

- ◆ The trTCM can be used to mark a IP packet stream in a service, where different, decreasing levels of assurances (either absolute or relative) are given to packets which are green, yellow, or red. Refer to RFC 2698 for more information on other aspects of trTCM.

Example

This example creates a policy called "rd-policy," uses the `class` command to specify the previously defined "rd-class," uses the `set phb` command to classify the service that incoming packets will receive, and then uses the **`police trtcm-color-blind`** command to limit the average bandwidth to 100,000 Kbps, the committed burst rate to 4000 bytes, the peak information rate to 1,000,000 kbps, the peak burst size

to 6000, to remark any packets exceeding the committed burst size, and to drop any packets exceeding the peak information rate.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set phb 3
Console(config-pmap-c)#police trtcm-color-blind 100000 4000 100000 6000
    conform-action transmit exceed-action 0 violate-action drop
Console(config-pmap-c)#
```

set cos This command modifies the class of service (CoS) value for a matching packet (as specified by the **match** command) in the packet's VLAN tag. Use the **no** form to remove this setting.

Syntax

[no] set cos *cos-value*

cos-value - Class of Service value. (Range: 0-7)

Default Setting

None

Command Mode

Policy Map Class Configuration

Command Usage

- ◆ The **set cos** command is used to set the CoS value in the VLAN tag for matching packets.
- ◆ The **set cos** and **set phb** command function at the same level of priority. Therefore setting either of these commands will overwrite any action already configured by the other command.

Example

This example creates a policy called "rd-policy," uses the **class** command to specify the previously defined "rd-class," uses the **set cos** command to classify the service that incoming packets will receive, and then uses the **police flow** command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4000 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set cos 3
Console(config-pmap-c)#police flow 10000 4000 conform-action transmit
    violate-action drop
Console(config-pmap-c)#
```

set phb This command services IP traffic by setting a per-hop behavior value for a matching packet (as specified by the [match](#) command) for internal processing. Use the **no** form to remove this setting.

Syntax

[no] set phb *phb-value*

phb-value - Per-hop behavior value. (Range: 0-7)

Default Setting

None

Command Mode

Policy Map Class Configuration

Command Usage

- ◆ The **set phb** command is used to set an internal QoS value in hardware for matching packets (see [Table 109, "Default Mapping of CoS/CFI to Internal PHB/Drop Precedence"](#)). The QoS label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion by the [police srtcm-color](#) command and [police trtcm-color](#) command.
- ◆ The [set cos](#) and **set phb** command function at the same level of priority. Therefore setting either of these commands will overwrite any action already configured by the other command.

Example

This example creates a policy called "rd-policy," uses the [class](#) command to specify the previously defined "rd-class," uses the **set phb** command to classify the service that incoming packets will receive, and then uses the [police flow](#) command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4000 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set phb 3
Console(config-pmap-c)#police flow 10000 4000 conform-action transmit
violate-action drop
Console(config-pmap-c)#
```


service-policy This command applies a policy map defined by the **policy-map** command to the ingress side of a particular interface. Use the **no** form to remove this mapping.

Syntax

[no] service-policy input *policy-map-name*

input - Apply to the input traffic.

policy-map-name - Name of the policy map for this interface.
(Range: 1-32 characters)

Default Setting

No policy map is attached to an interface.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ Only one policy map can be assigned to an interface.
- ◆ First define a class map, then define a policy map, and finally use the **service-policy** command to bind the policy map to the required interface.
- ◆ The switch does not allow a policy map to be bound to an interface for egress traffic.

Example

This example applies a service policy to an ingress interface.

```
Console(config)#interface ethernet 1/1
Console(config-if)#service-policy input rd-policy
Console(config-if)#
```

show class-map This command displays the QoS class maps which define matching criteria used for classifying traffic.

Syntax

show class-map [*class-map-name*]

class-map-name - Name of the class map. (Range: 1-32 characters)

Default Setting

Displays all class maps.

Command Mode

Privileged Exec

Example

```

Console#show class-map
Class Map match-any rd-class#1
Description:
  Match IP DSCP 10
  Match access-list rd-access
  Match IP DSCP 0

Class Map match-any rd-class#2
  Match IP Precedence 5

Class Map match-any rd-class#3
  Match VLAN 1

Console#

```

show policy-map This command displays the QoS policy maps which define classification criteria for incoming traffic, and may include policers for bandwidth limitations.

Syntax

show policy-map [*policy-map-name* [**class** *class-map-name*]]

policy-map-name - Name of the policy map. (Range: 1-32 characters)

class-map-name - Name of the class map. (Range: 1-32 characters)

Default Setting

Displays all policy maps and all classes.

Command Mode

Privileged Exec

Example

```

Console#show policy-map
Policy Map rd-policy
Description:
  class rd-class
  set phb 3
Console#show policy-map rd-policy class rd-class
Policy Map rd-policy
  class rd-class
    set phb 3
Console#

```

show policy-map interface This command displays the service policy assigned to the specified interface.

Syntax

show policy-map interface *interface* **input**

interface

unit/port

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Command Mode

Privileged Exec

Example

```
Console#show policy-map interface 1/5 input
Service-policy rd-policy
Console#
```


Data Center Bridging Commands

Fibre Channel was developed as a dedicated fabric that loses little to no packets, and was not designed to work on an unreliable network. For this reason, a set of standards termed Data Center Bridging (DCB) have been developed to increase the reliability of Ethernet-based networks in the data center. DCB consists of four different technologies: DCB Exchange (DCBX), Priority-based Flow Control (PFC), Enhanced Transmission Selection (ETS), and Congestion Notification (CN). These standards provide an effective method of speeding traffic through the data center.

Table 115: Data Center Bridging Commands

Command	Function
DCB Exchange	Provides the mechanism which allows peers to exchange configuration information via LLDP TLVs about ETS and PFC settings and their willingness to accept ETS configuration recommendations.
Priority-based Flow Control	Adds fields to the standard PAUSE frame that allow a device to inhibit the transmission of frames for certain priorities as opposed to inhibiting all frame transmissions.
Enhanced Transmission Selection	Allows the priorities used for services with similar bandwidth requirements to be combined into a traffic class group, and a minimum bandwidth set for each group.
Congestion Notification	CN is a mechanism to transmit congestion information on an end-to-end basis per traffic flow back to the edge of the network where the flow that causes the congestion can be easily isolated and rate limited.

DCB Exchange Commands

This section describes the commands used by DCB devices to exchange configuration information with directly-connected peers. These commands are also used to detect misconfiguration of the peer devices and, where accepted, to configured peer DCB devices.

Table 116: DCB Exchange Commands

Command	Function	Mode
dcbx	Enables DCBX on the selected interface	IC
dcbx mode	Configures DCBX mode used for message exchange	IC
show dcbx	Shows the DCBX configuration settings	PE

dcbx This command enables DCBX on the selected interface. Use the **no** form to disable DCBX.

Syntax

[no] dcbx

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ DCBX is normally deployed in FCoE topologies to support lossless operation for FCoE traffic. In these scenarios, all network elements are DCBX enabled. LLDP is also enabled on any port configured to use DCBX.
- ◆ DCBX uses LLDP to exchange attributes between two link peers. DCBX does this by exchanging LLDP TLVs with peer devices to discover DCB capabilities supported by a peer port, detect misconfiguration of a DCB feature between the peers on a link, and perform configuration of DCB features on its peer port if the peer port is willing to accept configuration settings. The configurable attributes include ETS recommendation, ETS Configuration, and PFC.
- ◆ DCBX operates over a point to point link. If multiple LLDP peer ports running DCBX are detected on an interface, then DCBX shall behave as if the peer port's DCBX TLVs are not present until the multiple LLDP peer port condition is no longer present.

Example

The following example enables DCBX on port 5:

```
Console(config)#interface ethernet 1/5
Console(config-if)#dcbx
Console(config-if)#
```

dcbx mode This command configures the DCBX mode used for message exchange. Use the **no** form to restore the default setting.

Syntax

dcbx mode {auto-down | auto-up | configuration-source | manual}

no dcbx mode

auto-down – In auto-downstream mode, the port advertises a configuration but is not willing to accept one from the link partner. However, it will accept a configuration propagated internally from the

configuration source. Selection of a port based upon compatibility of the received configuration is suppressed.

auto-up – In auto-upstream mode, the port advertises a configuration, but it is also willing to accept a configuration from the link-partner and propagate it internally to the auto-downstream ports, as well as receive a configuration propagated internally by other auto-upstream ports.

configuration-source – In configuration-source mode, the port is manually selected as the configuration source. A configuration received over this port is propagated to the other auto-downstream and auto-upstream ports.

manual – In manual mode, the port does not accept a configuration from peer devices, nor does it accept any internally propagated configuration. The operational mode, traffic classes, and bandwidth information must be specified by the operator. These ports will advertise their configuration to a peer if DCBX is enabled on that port.

Default Setting

Manual

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ Auto-downstream ports have the recommendation TLV parameter enabled. If these ports receive internally propagated information, they will utilize this information and ignore their local configuration.
- ◆ On auto-upstream ports, a recommendation TLV is sent to its peer, and processed if received locally. Auto-upstream ports that receive internally propagated information utilize this information and ignore their local configuration. The first auto-upstream port to successfully accept a compatible configuration becomes the configuration source.

Peer configurations received on auto-upstream ports other than the configuration source are accepted if compatible with the configuration source, and the DCBX client is set to operationally active on the auto-upstream port. If the configuration is not compatible with the configuration source, a message is logged indicating an incompatible configuration, an error counter incremented, and the DCBX client operationally disabled on the port.

- ◆ On a port set to configuration-source mode, automatic election of a new configuration source port is not allowed. Events that would cause selection of a new configuration source are ignored. The configuration received over the configuration source port is maintained until it is cleared by setting the port to the manual mode. Only the configuration source is allowed to propagate its configuration to other ports internally.

If no port is set to configuration-source mode, then the first auto-upstream port to accept a compatible configuration becomes the configuration source.

- ◆ On a port set to manual mode, only locally configured settings are used to construct DCBX TLVs. On these ports, the operational mode, traffic classes, and bandwidth information must be specified by the operator. These ports advertise their configuration to their peer if DCBX is enabled on that port. Any incompatible peer configurations received on these ports are logged and an error counter incremented.

Example

The following example sets DCBX mode to auto-upstream on port 5:

```
Console(config)#interface ethernet 1/5
Console(config-if)#dcbx mode auto-up
Console(config-if)#
```

show dcbx This command shows the DCBX configuration settings and status of the LLDP TLV willing bits.

Syntax

show dcbx [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Default Setting

Shows DCBX configuration settings for all ports.

Command Mode

Privileged Exec

Example

This example displays the DCBX administrative status, operational mode, and the status of the LLDP TLV willing bit for ETS and PFC.

```
Console#show dcbx ethernet 1/5
DCBX Port Configuration
  Port      Status   Mode                ETS Willing PFC Willing
  -----
  Eth 1/5   Enabled   AutoUpstream        No           No
Console#
```


Priority-based Flow Control Commands

Priority-based Flow Control (PFC) is used to reduce frame loss due to congestion by inhibiting the transmission of frames based on individual traffic classes. PFC can pause high priority traffic only when necessary to avoid dropping frames, while allowing traditional traffic assigned other priorities to continue flowing through an interface.

Traffic classes are specified in the priority field of the 802.1Q VLAN header, which identifies an 802.1p priority value. However, a VLAN unaware end station can also use PFC by sending traffic as priority-tagged and ignoring the VLAN ID in received frames. Note that some frames, such as BPDUs, are sent untagged and can bypass the output queues, it is strongly recommended that the default priority for a port not have PFC enabled.

PFC can reduce the number of frames discarded due to congestion for loss-sensitive protocols. However, PFC can cause congestion to spread, and is therefore intended for use on networks of limited extent, such as within a data center. When PFC is used, deployment of Congestion Notification (CN) can reduce the frequency at which PFC is invoked.

Table 117: Priority-based Flow Control Commands

Command	Function	Mode
<code>pfc mode</code>	Sets the PFC mode to negotiate capability through DCBX or by forcing it to on state	IC
<code>pfc priority</code>	Enables PFC for specified priorities	IC
<code>clear pfc statistics</code>	Clears PFC statistics	PE
<code>show pfc</code>	Shows PFC configuration settings	PE
<code>show pfc statistics</code>	Shows PFC statistics for the number of PFC frames received and transmitted for each priority	PE

Configuration Guidelines

Take the following steps to configure PFC:

1. Ensure that tagging is enabled on the interfaces using PFC so that the 802.1p priority values are carried through the network (using the `switchport allowed vlan` command).
2. Use the `pfc mode` command to enable priority-based flow control on the interface.
3. Use the `pfc priority` command to specify the CoS values that should be paused (i.e., not dropped) due to greater loss sensitivity.

pfc mode Use this command to sets the PFC mode to negotiate capability through DCBX or by forcing it to on state. Use the **no** form to disable this feature.

Syntax

pfc mode {auto | on}

no pfc mode

auto – Negotiates PFC capability using DCBX. The operational capability of PFC depends on the result of DCBX negotiations.

on – Forces PFC to enabled state

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ Operator configuration of PFC is used only when the port is configured in DCBX manual mode. When interoperating with other equipment in manual mode, the peer equipment must be configured with identical PFC priorities and VLAN assignments. Ports configured in auto-upstream or auto-downstream DCBX roles receive their PFC configuration from the configuration source and ignore any manually configured information. Interfaces not enabled for PFC ignore received PFC frames.
- ◆ PFC is configurable on full duplex interfaces only. To enable PFC on a LAG, the member interfaces must have the same configuration.
- ◆ When PFC is enabled on an interface, it will be automatically disabled for IEEE 802.3 flow control. Any flow control frames received on a PFC enabled interface are ignored. When PFC is disabled on an interface, it defaults to IEEE 802.3 flow control.

Example

The following example sets port 5 to use PFC auto-negotiation mode.

```
Console(config)#interface ethernet 1/5
Console(config-if)#pfc mode auto
Console(config-if)#
```

pfc priority Use this command to enable PFC for specified priorities. Use the **no** form to disable PFC for specified priorities.

Syntax

[no] pfc priority enable *priority-list*

priority-list – Priority identifier, specified as a single number, a range of consecutive numbers separated by a hyphen, or multiple numbers separated by commas. (Range: 0-7)

Default Setting

Enabled for CoS value 3

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ If a priority list has already been created by this command, then any priorities specified by subsequent commands are added to the existing list.
- ◆ When PFC is enabled, the interface will not pause any CoS priority frames unless there is at least one pause priority set by this command.
- ◆ Each priority is configured as drop (PFC disabled) or no-drop (PFC enabled). If a priority designated as no-drop is congested, that priority is paused. The same no-drop priorities must be configured across the network in order to ensure end-to-end lossless behavior. VLAN tagging also needs to be turned on in order to carry the PFC priority settings through the network.

Example

The following example configures port 4 to receive mirrored RSPAN traffic:

```
Console(config)#interface ethernet 1/5
Console(config-if)#pfc priority enable 3,5
Console(config-if)#
```

clear pfc statistics Use this command to clear PFC statistics.

Syntax

clear pfc statistics [**interface** *interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Default Setting

None

Command Mode

Privileged Exec

Example

This example clears PFC statistics on all interfaces.

```
Console#clear pfc statistics
Console#
```

show pfc Use this command to show PFC configuration settings.

Syntax

show pfc [**interface** *interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Command Mode

Privileged Exec

Example

This example displays the PFC administrative status, operational mode, and the priority bits for frames to pause (instead of drop) when congestion occurs in the specified priority buffers.

```
Console#show pfc interface ethernet 1/5
Interface Admin    Oper    Admin    Oper
          Mode     Mode    Enabled Pri    Enabled Pri
-----
Eth 1/ 5  Auto     Enabled  3                3
Console#
```

show pfc statistics Use this command to show PFC statistics for the number of PFC frames received and transmitted for each priority.

Syntax

show pfc statistics [**interface** *interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Command Mode

Privileged Exec

Example

This example shows the number of received and transmitted PFC frames for each priority class used for Port 5.

```
Console#show pfc statistics interface ethernet 1/5
Interface Pri Rx PFC Frames      Tx PFC Frames
-----
Eth 1/ 5   0                0                0
Eth 1/ 5   1                0                0
Eth 1/ 5   2                0                0
Eth 1/ 5   3                0                0
Eth 1/ 5   4                0                0
Eth 1/ 5   5                0                0
Eth 1/ 5   6                0                0
Eth 1/ 5   7                0                0

Console#
```

Enhanced Transmission Selection Commands

Enhanced Transmission Selection (ETS) provides a means to allocate link bandwidth to different priority groups as a percentage of total bandwidth. These settings are then advertised to other devices in a data center network through DCBX ETS TLVs. Peer devices accept ETS traffic class group and bandwidth information TLVs from auto-upstream devices and propagate it to auto-downstream devices.

The priority of a packet arriving at an interface is grouped into a TCG at the first level of scheduling, ensuring that the minimum bandwidth is provided. The packet is then steered into the appropriate outbound CoS queue through a mapping table by a second level scheduler. Using ETS, the required bandwidth is provided to each TCG. Within each TCG, multiple traffic classes share the bandwidth of the group.

Table 118: ETS Commands

Command	Function	Mode
<code>ets mode</code>	Sets the ETS mode to negotiate capability through DCBX or by forcing it to on state	IC
<code>traffic-class algo</code>	Sets the queue scheduling algorithm assigned to a traffic class group	IC
<code>traffic-class map</code>	Maps a given priority to a traffic class group	IC
<code>traffic-class weight</code>	Configures the bandwidth allocation for all TCGs	IC
<code>show ets mapping</code>	Displays priority to TCG mapping	PE
<code>show ets weight</code>	Displays the bandwidth allocation for selected TCGs	PE

Configuration Guidelines

Take the following steps to configure ETS:

1. Map CoS queues to TCGs for the egress ports using the `traffic-class map` command.
2. Configure the bandwidth allocation for all TCGs using the `traffic-class weight` command.
3. Enable the required scheduling algorithm for each TCG using the `traffic-class algo` command.
4. Ensure that the 802.1p priority present in the frames entering the ingress ports is set to be trusted using the `qos map trust-mode` command.
5. Set the ETS mode to auto-negotiation through DCBX or force it into on state using the `ets mode` command.

ets mode Use this command to set the ETS mode to negotiate capability through DCBX or by forcing it to on state. Use the no form to restore the default setting.

Syntax

ets mode {auto | on}

no ets mode

auto – Negotiates ETS capability using DCBX. The operational capability of ETS depends on the result of DCBX negotiations.

on – Forces ETS to enabled state.

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ Operator configuration of ETS is used only when the port is configured in DCBX manual mode. When interoperating with other equipment in manual mode, the peer equipment must be configured with identical ETS TCG queuing algorithm, priority queue mapping, and minimum bandwidth requirements. Ports configured in auto-upstream or auto-downstream DCBX roles receive their ETS configuration from the configuration source and ignore any manually configured information. Interfaces not enabled for ETS ignore received ETS frames.
- ◆ ETS is configurable on full duplex interfaces only. To enable ETS on a LAG, the member interfaces must have the same configuration.

Example

The following example sets port 5 to use ETX auto-negotiation mode.

```
Console(config)#interface ethernet 1/5
Console(config-if)#ets mode auto
Console(config-if)#
```

traffic-class algo Use this command to set the queue scheduling algorithm assigned to a traffic class group. Use the **no** form to restore the default setting.

Syntax

traffic-class algo {strict | ets}

no traffic-class algo

strict - Processes all packets entering this interface using strict priority.

ets - Processes packets with priority values specified for a TCG using Weighted Deficit Round Robin (WDRR).

Default Setting

strict

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

Packets with priority values not specified for a TCG use strict priority and therefore are processed ahead of the packets in the weighted queues.

Example

The following example sets the traffic-class algorithm for port 5 to use ETS.

```
Console(config)#interface ethernet 1/5
Console(config-if)#traffic-class algo ets
Console(config-if)#
```

traffic-class map Use this command to map a given priority to a traffic class group (TCG). Use the **no** form to restore the default mapping for a priority value.

Syntax

traffic-class map *priority traffic-class-group*

no traffic-class algo *priority*

priority - 802.1p priority value in ingress packets. (Range: 0-7)

traffic-class-group - The TCG to which packets with specified priorities are assigned. (Range: 0-2)

Default Setting

All priorities are mapped to TCG 0.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ One or more priorities may be assigned to a TCG using multiple commands.
- ◆ Interfaces where ETS is not enabled discard any received ETS TLVs.

Example

The following example maps priority 2 and 3 to TCG 0 for port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#traffic-class map 2 1
Console(config-if)#traffic-class map 3 1
Console(config-if)#
```


traffic-class weight Use this command to configure the bandwidth allocation for all TCGs on an interface. Use the **no** form to restore the default settings.

Syntax

traffic-class weight *weight1 weight2 weight3*

no traffic-class weight

weight1~3 - The percentage of bandwidth assigned to each TCG.
(Range: 0-100)

Default Setting

0

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ The cumulative weight for all three TCGs must be 100.
- ◆ The weight assigned by the **traffic-class weight** command must be 0 for any TCG set to strict mode with the **traffic-class algo** command.
- ◆ The weight for up to three TCGs may be defined. The bandwidth available to the TCGs is the maximum percentage of available link bandwidth after all of the packets with priorities configured for strict mode have been serviced. Once these have been processed, a TCG may only use available bandwidth up to the maximum percentage allocated by the **traffic-class weight** command. However, the unused bandwidth of any TCG may be shared by other TCGs.

Example

The following example sets the maximum bandwidth for TCGs 0-3 on port 5 to 25, 35, and 40 percent, respectively.

```
Console(config)#interface ethernet 1/5
Console(config-if)#traffic-class weight 25 35 40
Console(config-if)#
```

show ets mapping Use this command to display mapping from IEEE 802.1p priorities to the traffic class group (TCGs).

Syntax

show ets mapping [**interface** *interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Command Mode

Privileged Exec

Example

This example shows both the locally configured settings, and current operational settings.

```
Console#show ets mapping interface ethernet 1/5
Configuration:
ETS Mode: Auto
Priority Traffic Class
-----
      0      0
      1      0
      2      0
      3      0
      4      0
      5      0
      6      0
      7      0

Operational:
ETS Mode: On
Priority Traffic Class
-----
      0      0
      1      0
      2      0
      3      0
      4      0
      5      0
      6      0
      7      0

Console#
```

show ets weight Use this command to display the bandwidth allocation for selected TCGs.

Syntax

show ets mapping [**interface** *interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Command Mode

Privileged Exec

Example

This example shows both the locally configured settings, and current operational settings.

```

Console#show ets weight interface ethernet 1/5
Configuration:
ETS Mode: Auto
Traffic Class Tx Selection Mode Weight%
-----
          0 Strict                      0
          1 Strict                      0
          2 Strict                      0

Operational:
ETS Mode: On
Traffic Class Tx Selection Mode Weight%
-----
          0 Strict                      0
          1 Strict                      0
          2 Strict                      0

Console#

```

Congestion Notification Commands

Overview

If congestion is left uncontrolled, it can cause head-of-line blocking, and spread congestion across the network. Congestion Notification (CN) is a mechanism used to transmit congestion information on an end-to-end basis per traffic flow back to the edge of the network where the flow that causes the congestion can be easily isolated and rate limited.

When congestion notification is used, a congested switch (CP – Congestion Point) sends messages toward the source of the congestion (RP – Reaction Point) to signal

its congested state and that the rate of the flow entering the network should be reduced.

Upon receiving the CN messages, rate limiting is initiated as close as possible to the source of the congestion. This alleviates the congestion at the network core and stops it from spreading through the network.

Congestion Notification is different from PFC in that CN messages are propagated all the way toward the source of the congestion, while the PFC Pause is a hop-by-hop process, and normally takes longer to slow down the congestion caused by a specific flow.

The rate limiter parameters prompted by CN notifications are dynamically adjusted based on feedback coming from the CPs. CN functions at Layer 2 and therefore applies to all traffic types, using exponential decrease in traffic rates when congestion occurs, and a linear increase when bandwidth is available.

Congestion Notification Domains

Congestion notification depends on the formation of a cooperating set of network devices including VLAN-aware bridges and end stations to reduce frame loss. By partitioning the bridges' and end stations' resources, frames sourced or sunk by non-cooperating bridges or end stations can be carried across the network with minimal contention with Congestion Controlled Flows (CCFs) for those resources.

Operational Concept

In order for CN to successfully control congestion in a Virtual Bridged Network, the bridges and end stations in that network have to be configured with CN values that are appropriate to the characteristics of the CCFs generated by the applications that expect congestion controlled services. For example:

1. If frames that were not originated from an RP can enter a CP experiencing congestion, then the CNMs generated by that CP upon receipt of those frames cannot correct the problem.
2. Congestion notification cannot operate correctly if a CP's configuration is inappropriate for the CCFs passing through it, or if priority values are regenerated in a manner that moves frames in and out of CNPVs.
3. Frames transmitted from an end station with a CN-TAG cannot be understood by an end station that is not congestion aware.

Congestion aware bridges are therefore used to construct a Congestion Notification Domain (CND), within which a particular Congestion Notification Priority Value (CNPV) is supported. A CND is a connected subset of the bridges and end stations in a Virtual Bridged LAN that are configured to serve a particular CNPV. CNDs can be created by configuring the bridges and end stations in a network, or they can be created automatically, using an additional TLV element, the Congestion Notification TLV.

The QCN algorithm is composed of the following two parts:

1. Congestion Point (CP) Algorithm: This is the mechanism by which a congested bridge or end station buffer samples outgoing frames and generates a feedback message (CNM – Congestion Notification Message) addressed to the source of the sampled frame. The feedback message contains information about the extent of congestion at the CP.
2. Reaction Point (RP) Algorithm: This is the mechanism by which a Rate Limiter associated with a source decreases its sending rate based on feedback received from the CP, and increases its rate unilaterally (without further feedback) to recover lost bandwidth and probe for extra available bandwidth.

Table 119: CN Commands

Command	Function	Mode
<code>cn</code>	Enables congestion notification	GC
<code>cn cnm-transmit-priority</code>	Configures the dot1p priority used for transmitting any Congestion Notification Message (CNM)	GC
<code>cn cnpv</code>	Sets a dot1p priority to be a Congestion Notification Priority Value (CNPV)	GC
<code>cn cnpv alternate-priority</code>	Configures the alternate priority used to remark a received frame when its dot1p priority is equal to the CNPV when the defense mode is other than auto	GC
<code>cn cnpv defense-mode</code>	Configures the defense mode for a CNPV, determining whether CN is enabled or not, and if enabled, whether the port remarks the CNPV to a non-CNPV value on input, and whether the port removes CN-tags on output	GC
<code>cn cnpv alternate-priority</code>	Configures the alternate priority used to remark a received frame when its dot1p priority is equal to the CNPV when the defense mode is other than auto	IC
<code>cn cnpv defense-mode</code>	Configures the defense mode for a CNPV, determining whether CN is enabled or not, and if enabled, whether the port remarks the CNPV to a non-CNPV value on input, and whether the port removes CN-tags on output	IC
<code>show cn</code>	Shows the global CN status	PE
<code>show cn cnpv</code>	Shows CNPV information, including defense mode and alternate priority	PE
<code>show cn cp</code>	Shows functional settings and status for the specified CP	PE

- cn** Use this command to enable congestion notification for all ports on the switch. Use the **no** form to disabled congestion notification on the switch.

Syntax

[no] cn

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

When CN is enabled, the system recognizes the CN-TAG in received frames, the Connection Point (CP) algorithm and Reaction Points (RP) algorithm runs on the configured CPs and Congestion Notification Messages (CNMs) are transmitted if congestion is detected on a CP.

Example

The following example enables CN for all ports.

```
Console(config)#interface ethernet 1/5
Console(config-if)#traffic-class map 2 1
Console(config-if)#traffic-class map 3 1
Console(config-if)#
```

- cn cnm-transmit-priority** Use this command to configure the dot1p priority used for transmitting any Congestion Notification Message (CNM). Use the **no** form to restore the default setting.

Syntax

cn cnm-transmit-priority *priority*

no cn cnm-transmit-priority

priority - dot1p priority used to transmit any CNM. (Range: 0-7)

Default Setting

0

Command Mode

Global Configuration

Command Usage

The specified priority should not be equal to any existing Congestion Notification Priority Value (CNPV).

Example

The following example sets the CNM transmit priority to 1.

```
Console(config)#cn cnm-transmit-priority 1
Console(config)#
```

cn cnpv Use this command to set a dot1p priority to be a Congestion Notification Priority Value (CNPV). Use the **no** form to change a CNPV back to a dot1p priority value.

Syntax

[no] cn cnpv cnpv-priority

cnpv-priority - CNPV assigned to Congestion Control Flows (CFF) on this port. (Range: 0-7)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ Up to 7 CNPVs can be set for the system.
- ◆ When a CNPV is changed to be non-CNPV using the **no** form of this command, other CNPVs which are not administratively disabled on a port may be operationally enabled if the operational defense mode is still disabled.
- ◆ When the number of CPs reaches the maximum for a port, the operational defense mode for related CNPVs on that port is disabled.

Example

The following example sets a CNPV to 2.

```
Console(config)#cn cnpv 2
Console(config)#
```

cn cnpv Use this command to configure the alternate priority used to remark a received
alternate-priority frame when its dot1p priority is equal to the CNPV when the defense mode is other
(Global Configuration) than auto. Use the **no** form restore the default setting.

Syntax

cn cnpv *cnpv-priority* **alternate-priority** *priority*

no cn cnpv *cnpv-priority* **alternate-priority**

cnpv-priority - CN priority value. (Range: 0-7)

priority - Remarkd priority value. (Range: 0-7)

Default Setting

Alternate Priority: 0

Command Mode

Global Configuration

Command Usage

- ◆ Use the alternate priority to steer away traffic that comes from congestion unaware sources. Traffic from CN unaware sources should be remarked when entering the CN domain so that resources assigned to the CN-enabled queues are not exhausted with traffic from CN unaware sources. Frames coming from non-CN sources do not have a CN-TAG. If these frames are mapped to the CN-enabled queue, then they may contribute to the congestion and trigger generation of CNMs. These messages are not useful to sources that are CN unaware.
- ◆ If a port's neighbor is known to be configured for a particular CNPV, the entry in the port's priority regeneration table for that CNPV is ignored, and the priority is never changed on input.
- ◆ If a port's neighbor is known to not be configured for a particular CNPV configured on this port, the entry in the port's priority regeneration table for that CNPV shall be overridden to translate the CNPV to an alternate non-CNPV value.
- ◆ If a CNPV is configured on any port, then on that port, the port's priority regeneration table shall be overridden to prevent any other priority value from being remapped into that CNPV.

Example

The following example maps CNPV 2 to alternate priority 5.

```
Console(config)#cn cnpv 2 alternate-priority 5
Console(config)#
```


cn cnpv defense-mode (Global Configuration) Use this command to configure the defense mode for a CNPV, determining whether CN is enabled or not, and if enabled, whether the port remarks the CNPV to a non-CNPV value on input, and whether the port removes CN-tags on output. Use the **no** form to restore the default settings.

Syntax

cn cnpv cnpv-priority defense-mode {auto | disabled | edge | interior | interior-ready}

no cn cnpv cnpv-priority defense-mode

cnpv-priority - CN priority value. (Range: 0-7)

auto - Defense mode and alternate priority is chosen automatically as determined by the LLDP Congestion Notification TLV.

disabled - CN capability is administratively disabled.

edge - CNPV is remapped to non-CNPV and CN-TAG is removed.

interior - Priority remapping is inhibited and CN-TAG is removed.

interior-ready - Priority remapping is inhibited and CN-TAG is retained.

Default Setting

auto

Command Mode

Global Configuration

Command Usage

- ◆ Under the **auto** option, the defense mode is determined by the LLDP CN TLV, and may be set to edge, interior, or interior-ready.

The alternate priority is also determined by the LLDP CN TLV. If CN is enabled and the CND defense mode of the port is Edge, then the CNPV to which an incoming frame can be mapped is the next lower priority value which is not mapped as a CNPV, or the next higher non-CNPV, if all lower values are CNPVs.

- ◆ Under the **disabled** option, the congestion notification capability is administratively disabled for this priority value and port. The priority regeneration table controls the remapping of input frames on this port to or from this priority. CN-TAGs are not stripped by the switch.
- ◆ Under the **edge** option, on this port and for this CNPV, the priority parameters of input frames are remapped to an alternate (non-CNPV) value, and no priority value is remapped to this CNPV regardless of the priority regeneration table. CN-TAGs are removed from frames before being output by the switch.
- ◆ Under the **interior** option, on this port and for this CNPV, the priority parameters of input frames are not remapped to another value, and no priority value is remapped to this CNPV, regardless of the priority regeneration table. CN-TAGs are removed from frames before being output by the switch.

- ◆ Under the **interior-ready** option, on this port and for this CNPV, the priority parameters of input frames are not remapped to another value, and no priority value is remapped to this CNPV, regardless of the priority regeneration table. CN-TAGs are not removed from frames by the switch.

Example

The following example sets the defense mode to edge for CNPV 2.

```
Console(config)#cn cnpv 2 defense-mode edge
Console(config)#
```

cn cnpv alternate-priority (Interface Configuration)

Use this command to configure the alternate priority used to remark a received frame when its dot1p priority is equal to the CNPV when the defense mode is other than auto. Use the **no** form to use the global setting for the CNPV.

Syntax

cn cnpv *cnpv-priority* **alternate-priority** *priority*

no cn cnpv *cnpv-priority* **alternate-priority**

cnpv-priority - CN priority value. (Range: 0-7)

priority - Remarkd priority value. (Range: 0-7)

Default Setting

The CNPV to alternate priority mapping is based on the global setting configured by the [cn cnpv alternate-priority](#) (Global Configuration) command.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

Refer to the Command Usage section under the [cn cnpv alternate-priority](#) (Global Configuration) command for more information on this command.

Example

The following example maps CNPV 2 to alternate priority 5.

```
Console(config)#cn cnpv 2 alternate-priority 5
Console(config)#
```

cn cnpv defense-mode (Interface Configuration) Use this command to configure the defense mode for a CNPV, determining whether CN is enabled or not, and if enabled, whether the port remarks the CNPV to a non-CNPV value on input, and whether the port removes CN-tags on output. Use the **no** form to restore the default settings.

Syntax

cn cnpv cnpv-priority defense-mode {auto | disabled | edge | interior | interior-ready}

no cn cnpv cnpv-priority defense-mode

cnpv-priority - CN priority value. (Range: 0-7)

auto - Defense mode and alternate priority is chosen automatically as determined by the LLDP Congestion Notification TLV.

disabled - CN capability is administratively disabled.

edge - CNPV is remapped to non-CNPV and CN-TAG is removed.

interior - Priority remapping is inhibited and CN-TAG is removed.

interior-ready - Priority remapping is inhibited and CN-TAG is retained.

Default Setting

The CNPV to alternate priority mapping is based on the global setting configured by the **cn cnpv defense-mode** (Global Configuration) command.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

Refer to the Command Usage section under the **cn cnpv defense-mode** (Global Configuration) command for more information on this command.

Example

The following example sets the defense mode to edge for CNPV 2.

```
Console(config)#cn cnpv 2 defense-mode edge
Console(config)#
```

show cn Use this command to show the global CN status.

Syntax

show cn

Command Mode

Privileged Exec

Example

This example shows the global settings for congestion notification, and the number of discarded frames.

```
Console#show cn
Congestion Notification Global Information
Admin Status           : Enabled
Oper Status            : Enabled
CNM Transmit Priority  : 1
Total Discarded Frames : 0

Console#
```

show cn cnpv Use this command to show CNPV information, including the defense mode and alternate priority.

Syntax

show cn cnpv [*cnpv-priority*] [*interface*]

cnpv-priority - CN priority value. (Range: 0-7)

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Command Mode

Privileged Exec

Example

This example shows information for CNPV 0 on port 5.

```
Console#show cn cnpv 0 ethernet 1/5
Congestion Notification Per-CNPV Port Information
CNPV           : 0
Port           : Eth 1/5
Admin Defense Mode : By-Global
Oper Defense Mode  : Edge
Admin Alternate Priority : By-Global
Oper Alternate Priority  : 1

Console#
```

show cn cp Use this command to show functional settings and status for the specified CP.

Syntax

```
show cn cp interface index index
           interface
           ethernet unit/port
                   unit - Unit identifier. (Range: 1)
                   port - Port number. (Range: 1-52)
           port-channel channel-id (Range: 1-8)
           index - Congestion Point index. (Range: 0-1)
```

Command Mode

Privileged Exec

Example

This example shows information for CP 0 on port 5.

```
Console#sh cn cp ethernet 1/5 index 0
Congestion Notification Per-Port Per-CP Information
Port                : Eth 1/5
CP Index            : 0
CPID                : 0012CF0105000500
Queue               : 2
Managed CNPVs      : 0
MAC Address         : 70-72-CF-8C-2F-EF
Set Point           : 26000
Feedback Weight     : 2
Minimum Sample Base : 150000 bytes
Discarded Frames    : 0
Transmitted Frames  : 0
Transmitted CNMs    : 0

Console#
```

Table 120: show cn cp - display description

Field	Description
Port	Port identifier.
CP Index	This index is used to distinguish between unique flows since more than one Congestion Notification Priority Value (CNPV) can flow through a single CP.
CPID	A number that, along with the source address and VLAN identifier of a CNM PDU, uniquely identifies a CP in a Virtual Bridged Network
Queue	The priority queue assigned to this CNPV.
Managed CNPVs	The number of CNPVs assigned to this congestion point. (Range: 0-2)
MAC Address	MAC address, belonging to the system transmitting the CNM PDU, used as the source address of Congestion Notification Messages (CNMs) sent from this CP.

Table 120: show cn cp - display description (Continued)

Field	Description
Set Point	The set-point for the queue. This is the target number of octets in the CP's queue. (Default: 26000)
Feedback Weight	Variable used in calculation of Quantized Feedback and New Sample Base. If the queue length is moving toward the set point, the feedback weight will be closer to 0 than if the queue length is moving away from the set point.
Minimum Sample Base	The minimum number of octets to enqueue in the CP's queue between CNM PDU transmissions. (Default: 150,000 bytes)
Discarded Frames	The number of frames offered to this CP that were discarded because of a full output queue.
Transmitted Frames	The number of data frames enqueued for transmission on this CP's output queue.
Transmitted CNMs	The number of CNMs transmitted by this CP.

Multicast Filtering Commands

This switch uses IGMP (Internet Group Management Protocol) to check for any attached hosts that want to receive a specific multicast service. It identifies the ports containing hosts requesting a service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.

Note that IGMP query can be enabled globally at Layer 2, or enabled for specific VLAN interfaces at Layer 3. (Layer 2 query is disabled if Layer 3 query is enabled.)

Table 121: Multicast Filtering Commands

Command Group	Function
IGMP Snooping	Configures multicast groups via IGMP snooping or static assignment, sets the IGMP version, enables proxy reporting, displays current snooping settings, and displays the multicast service and group members
Static Multicast Routing	Configures static multicast router ports which forward all inbound multicast traffic to the attached VLANs
IGMP Filtering and Throttling	Configures IGMP filtering and throttling
MLD Snooping	Configures multicast snooping for IPv6
MVR for IPv4	Configures a single network-wide multicast VLAN shared by hosts residing in other standard or private VLAN groups, preserving security and data isolation for normal traffic
MVR for IPv6	Configures a single network-wide multicast VLAN shared by hosts residing in other standard or private VLAN groups, preserving security and data isolation for normal traffic
IGMP (Layer 3)	Configures the IGMP protocol used with multicast routing in IPv4 networks
IGMP Proxy Routing	Collects and sends multicast group membership information onto the upstream interface based on IGMP messages monitored on downstream interfaces, and forwards multicast traffic based on that information
MLD (Layer 3)	Configures the MLD protocol used with multicast routing in IPv6 networks
MLD Proxy Routing	Collects and sends multicast group membership information onto the upstream interface based on MLD messages monitored on downstream interfaces, and forwards multicast traffic based on that information

IGMP Snooping

This section describes commands used to configure IGMP snooping on the switch.

Table 122: IGMP Snooping Commands

Command	Function	Mode
<code>ip igmp snooping</code>	Enables IGMP snooping	GC
<code>ip igmp snooping proxy-reporting</code>	Enables IGMP Snooping with Proxy Reporting	GC
<code>ip igmp snooping querier</code>	Allows this device to act as the querier for IGMP snooping	GC
<code>ip igmp snooping router-alert-option-check</code>	Discards any IGMPv2/v3 packets that do not include the Router Alert option	GC
<code>ip igmp snooping router-port-expire-time</code>	Configures the querier timeout	GC
<code>ip igmp snooping tcn-flood</code>	Floods multicast traffic when a Spanning Tree topology change occurs	GC
<code>ip igmp snooping tcn-query-solicit</code>	Sends an IGMP Query Solicitation when a Spanning Tree topology change occurs	GC
<code>ip igmp snooping unregistered-data-flood</code>	Floods unregistered multicast traffic into the attached VLAN	GC
<code>ip igmp snooping unsolicited-report-interval</code>	Specifies how often the upstream interface should transmit unsolicited IGMP reports (when proxy reporting is enabled)	GC
<code>ip igmp snooping version</code>	Configures the IGMP version for snooping	GC
<code>ip igmp snooping version-exclusive</code>	Discards received IGMP messages which use a version different to that currently configured	GC
<code>ip igmp snooping vlan general-query-suppression</code>	Suppresses general queries except for ports attached to downstream multicast hosts	GC
<code>ip igmp snooping vlan immediate-leave</code>	Immediately deletes a member port of a multicast service if a leave packet is received at that port and immediate-leave is enabled for the parent VLAN	GC
<code>ip igmp snooping vlan last-memb-query-count</code>	Configures the number of IGMP proxy query messages that are sent out before the system assumes there are no local members	GC
<code>ip igmp snooping vlan last-memb-query-intvl</code>	Configures the last-member-query interval	GC
<code>ip igmp snooping vlan mrd</code>	Sends multicast router solicitation messages	GC
<code>ip igmp snooping vlan proxy-address</code>	Configures a static address for proxy IGMP query and reporting	GC
<code>ip igmp snooping vlan proxy-reporting</code>	Enables IGMP Snooping with Proxy Reporting	GC
<code>ip igmp snooping vlan query-interval</code>	Configures the interval between sending IGMP general queries	GC
<code>ip igmp snooping vlan query-resp-intvl</code>	Configures the maximum time the system waits for a response to general queries	GC
<code>ip igmp snooping vlan static</code>	Adds an interface as a member of a multicast group	GC

Table 122: IGMP Snooping Commands (Continued)

Command	Function	Mode
<code>ip igmp snooping</code> <code>vlan version</code>	Configures the IGMP version for snooping	GC
<code>ip igmp snooping</code> <code>vlan version-exclusive</code>	Discards received IGMP messages which use a version different to that currently configured	GC
<code>clear ip igmp snooping</code> <code>groups dynamic</code>	Clears multicast group information dynamically learned through IGMP snooping	PE
<code>clear ip igmp snooping</code> <code>statistics</code>	Clears IGMP snooping statistics	PE
<code>show ip igmp snooping</code>	Shows the IGMP snooping, proxy, and query configuration	PE
<code>show ip igmp snooping</code> <code>group</code>	Shows known multicast group, source, and host port mapping	PE
<code>show ip igmp snooping</code> <code>mrouter</code>	Shows multicast router ports	PE
<code>show ip igmp snooping</code> <code>statistics</code>	Shows IGMP snooping protocol statistics for the specified interface	PE

ip igmp snooping This command enables IGMP snooping globally on the switch or on a selected VLAN interface. Use the **no** form to disable it.

Syntax

[no] ip igmp snooping [vlan *vlan-id*]
vlan-id - VLAN ID (Range: 1-4094)

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

- ◆ When IGMP snooping is enabled globally, the per VLAN interface settings for IGMP snooping take precedence.
- ◆ When IGMP snooping is disabled globally, snooping can still be configured per VLAN interface, but the interface settings will not take effect until snooping is re-enabled globally.

Example

The following example enables IGMP snooping globally.

```
Console(config)#ip igmp snooping
Console(config)#
```

ip igmp snooping proxy-reporting This command enables IGMP Snooping with Proxy Reporting. Use the **no** form to restore the default setting.

Syntax

[no] ip igmp snooping proxy-reporting

ip igmp snooping vlan *vlan-id* proxy-reporting {enable | disable}

no ip igmp snooping vlan *vlan-id* proxy-reporting -

vlan-id - VLAN ID (Range: 1-4094)

enable - Enable on the specified VLAN.

disable - Disable on the specified VLAN.

Default Setting

Global: Enabled

VLAN: Based on global setting

Command Mode

Global Configuration

Command Usage

- ◆ When proxy reporting is enabled with this command, the switch performs "IGMP Snooping with Proxy Reporting" (as defined in DSL Forum TR-101, April 2006), including last leave, and query suppression. Last leave sends out a proxy query when the last member leaves a multicast group, and query suppression means that specific queries are not forwarded from an upstream multicast router to hosts downstream from this device.
- ◆ If the IGMP proxy reporting is configured on a VLAN, this setting takes precedence over the global configuration.

Example

```
Console(config)#ip igmp snooping proxy-reporting
Console(config)#
```

ip igmp snooping querier This command enables the switch as an IGMP querier. Use the **no** form to disable it.

Syntax

[no] ip igmp snooping querier

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

- ◆ IGMP snooping querier is not supported for IGMPv3 snooping (see [ip igmp snooping version](#)).
- ◆ If enabled, the switch will serve as querier if elected. The querier is responsible for asking hosts if they want to receive multicast traffic.

Example

```
Console(config)#ip igmp snooping querier
Console(config)#
```

ip igmp snooping router-alert-option- check

This command discards any IGMPv2/v3 packets that do not include the Router Alert option. Use the **no** form to ignore the Router Alert Option when receiving IGMP messages.

Syntax

[no] ip igmp snooping router-alert-option-check

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

As described in Section 9.1 of RFC 3376 for IGMP Version 3, the Router Alert Option can be used to protect against DOS attacks. One common method of attack is launched by an intruder who takes over the role of querier, and starts overloading multicast hosts by sending a large number of group-and-source-specific queries, each with a large source list and the Maximum Response Time set to a large value.

To protect against this kind of attack, (1) routers should not forward queries. This is easier to accomplish if the query carries the Router Alert option. (2) Also, when the switch is acting in the role of a multicast host (such as when using proxy routing), it should ignore version 2 or 3 queries that do not contain the Router Alert option.

Example

```
Console(config)#ip igmp snooping router-alert-option-check
Console(config)#
```

ip igmp snooping router-port-expire-time This command configures the querier timeout. Use the **no** form to restore the default.

Syntax

ip igmp snooping router-port-expire-time *seconds*

no ip igmp snooping router-port-expire-time

seconds - The time the switch waits after the previous querier stops before it considers it to have expired. (Range: 1-65535;
Recommended Range: 300-500)

Default Setting

300 seconds

Command Mode

Global Configuration

Example

The following shows how to configure the timeout to 400 seconds:

```
Console(config)#ip igmp snooping router-port-expire-time 400
Console(config)#
```

ip igmp snooping tcn-flood This command enables flooding of multicast traffic if a spanning tree topology change notification (TCN) occurs. Use the **no** form to disable flooding.

Syntax

[no] ip igmp snooping tcn-flood

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ When a spanning tree topology change occurs, the multicast membership information learned by the switch may be out of date. For example, a host linked to one port before the topology change (TC) may be moved to another port after the change. To ensure that multicast data is delivered to all receivers, by default, a switch in a VLAN (with IGMP snooping enabled) that receives a Bridge Protocol Data Unit (BPDU) with the TC bit set (by the root bridge) will enter into "multicast flooding mode" for a period of time until the topology has stabilized and the new locations of all multicast receivers are learned.

- ◆ If a topology change notification (TCN) is received, and all the uplink ports are subsequently deleted, a timeout mechanism is used to delete all of the currently learned multicast channels.
- ◆ When a new uplink port starts up, the switch sends unsolicited reports for all current learned channels out through the new uplink port.
- ◆ By default, the switch immediately enters into “multicast flooding mode” when a spanning tree topology change occurs. In this mode, multicast traffic will be flooded to all VLAN ports. If many ports have subscribed to different multicast groups, flooding may cause excessive loading on the link between the switch and the end host. Flooding may be disabled to avoid this, causing multicast traffic to be delivered only to those ports on which multicast group members have been learned.
- ◆ When the spanning tree topology changes, the root bridge sends a proxy query to quickly re-learn the host membership/port relations for multicast channels. The root bridge also sends an unsolicited Multicast Router Discover (MRD) request to quickly locate the multicast routers in this VLAN.

The proxy query and unsolicited MRD request are flooded to all VLAN ports except for the receiving port when the switch receives such packets.

Example

The following example enables TCN flooding.

```
Console(config)#ip igmp snooping tcn-flood
Console(config)#
```

ip igmp snooping tcn-query-solicit

This command instructs the switch to send out an IGMP general query solicitation when a spanning tree topology change notification (TCN) occurs. Use the **no** form to disable this feature.

Syntax

[no] ip igmp snooping tcn-query-solicit

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ When the root bridge in a spanning tree receives a topology change notification for a VLAN where IGMP snooping is enabled, it issues a global IGMP leave message (query solicitation). When a switch receives this solicitation, it floods it to all ports in the VLAN where the spanning tree change occurred.

When an upstream multicast router receives this solicitation, it will also immediately issues an IGMP general query.

- ◆ The **ip igmp snooping tcn query-solicit** command can be used to send a query solicitation whenever it notices a topology change, even if the switch is not the root bridge in the spanning tree.

Example

The following example instructs the switch to issue an IGMP general query whenever it receives a spanning tree topology change notification.

```
Console(config)#ip igmp snooping tcn query-solicit
Console(config)#
```

ip igmp snooping unregistered-data- flood

This command floods unregistered multicast traffic into the attached VLAN. Use the **no** form to drop unregistered multicast traffic.

Syntax

[no] ip igmp snooping unregistered-data-flood

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

Once the table used to store multicast entries for IGMP snooping and multicast routing is filled, no new entries are learned. If no router port is configured in the attached VLAN, and unregistered-flooding is disabled, any subsequent multicast traffic not found in the table is dropped, otherwise it is flooded throughout the VLAN.

Example

```
Console(config)#ip igmp snooping unregistered-data-flood
Console(config)#
```

ip igmp snooping unsolicited-report-interval This command specifies how often the upstream interface should transmit unsolicited IGMP reports when proxy reporting is enabled. Use the **no** form to restore the default value.

Syntax

ip igmp snooping unsolicited-report-interval *seconds*

no ip igmp snooping version-exclusive

seconds - The interval at which to issue unsolicited reports.
(Range: 1-65535 seconds)

Default Setting

400 seconds

Command Mode

Global Configuration

Command Usage

- ◆ When a new upstream interface (that is, uplink port) starts up, the switch sends unsolicited reports for all currently learned multicast channels out through the new upstream interface.
- ◆ This command only applies when proxy reporting is enabled (see [page 594](#)).

Example

```
Console(config)#ip igmp snooping unsolicited-report-interval 5
Console(config)#
```

ip igmp snooping version This command configures the IGMP snooping version. Use the **no** form to restore the default.

Syntax

ip igmp snooping [**vlan** *vlan-id*] **version** {**1** | **2** | **3**}

no ip igmp snooping version

vlan-id - VLAN ID (Range: 1-4094)

1 - IGMP Version 1

2 - IGMP Version 2

3 - IGMP Version 3

Default Setting

Global: IGMP Version 2

VLAN: Not configured, based on global setting

Command Mode

Global Configuration

Command Usage

- ◆ This command configures the IGMP report/query version used by IGMP snooping. Versions 1 - 3 are all supported, and versions 2 and 3 are backward compatible, so the switch can operate with other devices, regardless of the snooping version employed.
- ◆ If the IGMP snooping version is configured on a VLAN, this setting takes precedence over the global configuration.

Example

The following configures the global setting for IGMP snooping to version 1.

```
Console(config)#ip igmp snooping version 1
Console(config)#
```

ip igmp snooping version-exclusive

This command discards any received IGMP messages (except for multicast protocol packets) which use a version different to that currently configured by the [ip igmp snooping version](#) command. Use the **no** form to disable this feature.

Syntax

ip igmp snooping [vlan *vlan-id*] version-exclusive

no ip igmp snooping version-exclusive

vlan-id - VLAN ID (Range: 1-4094)

Default Setting

Global: Disabled

VLAN: Disabled

Command Mode

Global Configuration

Command Usage

- ◆ If version exclusive is disabled on a VLAN, then this setting is based on the global setting. If it is enabled on a VLAN, then this setting takes precedence over the global setting.
- ◆ When this function is disabled, the currently selected version is backward compatible (see the [ip igmp snooping version](#) command).

Example

```
Console(config)#ip igmp snooping version-exclusive
Console(config)#
```


ip igmp snooping vlan general-query-suppression This command suppresses general queries except for ports attached to downstream multicast hosts. Use the **no** form to flood general queries to all ports except for the multicast router port.

Syntax

[no] ip igmp snooping vlan *vlan-id* general-query-suppression

vlan-id - VLAN ID (Range: 1-4094)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ By default, general query messages are flooded to all ports, except for the multicast router through which they are received.
- ◆ If general query suppression is enabled, then these messages are forwarded only to downstream ports which have joined a multicast service.

Example

```
Console(config)#ip igmp snooping vlan 1 general-query-suppression
Console(config)#
```

ip igmp snooping vlan immediate-leave This command immediately deletes a member port of a multicast service if a leave packet is received at that port and immediate-leave is enabled for the parent VLAN. Use the **no** form to restore the default.

Syntax

[no] ip igmp snooping vlan *vlan-id* immediate-leave

vlan-id - VLAN ID (Range: 1-4094)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ If immediate-leave is *not* used, a multicast router (or querier) will send a group-specific query message when an IGMPv2/v3 group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the timeout period. (The timeout for this release is currently defined by `ip igmp snooping vlan last-memb-query-intvl` * `ip igmp robustval`.)

- ◆ If immediate-leave is enabled, the switch assumes that only one host is connected to the interface. Therefore, immediate leave should only be enabled on an interface if it is connected to only one IGMP-enabled device, either a service host or a neighbor running IGMP snooping.
- ◆ This command is only effective if IGMP snooping is enabled, and IGMPv2 or IGMPv3 snooping is used.

Example

The following shows how to enable immediate leave.

```
Console(config)#ip igmp snooping vlan 1 immediate-leave
Console(config)#
```

ip igmp snooping vlan last-memb-query- count

This command configures the number of IGMP proxy group-specific or group-and-source-specific query messages that are sent out before the system assumes there are no more local members. Use the **no** form to restore the default.

Syntax

ip igmp snooping vlan *vlan-id* last-memb-query-count *count*

no ip igmp snooping vlan *vlan-id* last-memb-query-count

vlan-id - VLAN ID (Range: 1-4094)

count - The number of proxy group-specific or group-and-source-specific query messages to issue before assuming that there are no more group members. (Range: 1-255)

Default Setting

2

Command Mode

Global Configuration

Command Usage

This command will take effect only if IGMP snooping proxy reporting or IGMP querier is enabled ([page 594](#)).

Example

```
Console(config)#ip igmp snooping vlan 1 last-memb-query-count 7
Console(config)#
```

ip igmp snooping vlan last-memb-query-intvl This command configures the last-member-query interval. Use the **no** form to restore the default.

Syntax

ip igmp snooping vlan *vlan-id* last-memb-query-intvl *interval*

no ip igmp snooping vlan *vlan-id* last-memb-query-intvl

vlan-id - VLAN ID (Range: 1-4094)

interval - The interval to wait for a response to a group-specific or group-and-source-specific query message. (Range: 1-31744 tenths of a second)

Default Setting

10 (1 second)

Command Mode

Global Configuration

Command Usage

- ◆ When a multicast host leaves a group, it sends an IGMP leave message. When the leave message is received by the switch, it checks to see if this host is the last to leave the group by sending out an IGMP group-specific or group-and-source-specific query message, and starts a timer. If no reports are received before the timer expires, the group record is deleted, and a report is sent to the upstream multicast router.
- ◆ A reduced value will result in reduced time to detect the loss of the last member of a group or source, but may generate more bursty traffic.
- ◆ This command will take effect only if IGMP snooping proxy reporting is enabled ([page 594](#)).

Example

```
Console(config)#ip igmp snooping vlan 1 last-memb-query-intvl 700
Console(config)#
```

ip igmp snooping vlan mrd This command enables sending of multicast router solicitation messages. Use the **no** form to disable these messages.

Syntax

[no] ip igmp snooping vlan *vlan-id* mrd

vlan-id - VLAN ID (Range: 1-4094)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ Multicast Router Discovery (MRD) uses multicast router advertisement, multicast router solicitation, and multicast router termination messages to discover multicast routers. Devices send solicitation messages in order to solicit advertisement messages from multicast routers. These messages are used to discover multicast routers on a directly attached link. Solicitation messages are also sent whenever a multicast forwarding interface is initialized or re-initialized. Upon receiving a solicitation on an interface with IP multicast forwarding and MRD enabled, a router will respond with an advertisement.
- ◆ Advertisements are sent by routers to advertise that IP multicast forwarding is enabled. These messages are sent unsolicited periodically on all router interfaces on which multicast forwarding is enabled. They are sent upon the expiration of a periodic timer, as a part of a router's start up procedure, during the restart of a multicast forwarding interface, and on receipt of a solicitation message. When the multicast services provided to a VLAN is relatively stable, the use of solicitation messages is not required and may be disabled using the **no ip igmp snooping vlan mrd** command.
- ◆ This command may also be used to disable multicast router solicitation messages when the upstream router does not support MRD, to reduce the loading on a busy upstream router, or when IGMP snooping is disabled in a VLAN.

Example

This example disables sending of multicast router solicitation messages on VLAN 1.

```
Console(config)#no ip igmp snooping vlan 1 mrd
Console(config)#
```

ip igmp snooping vlan proxy-address This command configures a static source address for locally generated query and report messages used by IGMP proxy reporting. Use the **no** form to restore the default source address.

Syntax

[no] ip igmp snooping vlan *vlan-id* proxy-address *source-address*

vlan-id - VLAN ID (Range: 1-4094)

source-address - The source address used for proxied IGMP query and report, and leave messages. (Any valid IP unicast address)

Default Setting

0.0.0.0

Command Mode

Global Configuration

Command Usage

IGMP Snooping uses a null IP address of 0.0.0.0 for the source of IGMP query messages which are proxied to downstream hosts to indicate that it is not the elected querier, but is only proxying these messages as defined in RFC 4541. The switch also uses a null address in IGMP reports sent to upstream ports.

Many hosts do not implement RFC 4541, and therefore do not understand query messages with the source address of 0.0.0.0. These hosts will therefore not reply to the queries, causing the multicast router to stop sending traffic to them.

To resolve this problem, the source address in proxied IGMP query and report messages can be replaced with any valid unicast address (other than the router's own address) using this command.

Rules Used for Proxy Reporting

When IGMP Proxy Reporting is disabled, the switch will use a null IP address for the source of IGMP query and report messages unless a proxy query address has been set.

When IGMP Proxy Reporting is enabled, the source address is based on the following criteria:

- ◆ If a proxy query address is configured, the switch will use that address as the source IP address in general and group-specific query messages sent to downstream hosts, and in report and leave messages sent upstream from the multicast router port.
- ◆ If a proxy query address is not configured, the switch will use the VLAN's IP address as the IP source address in general and group-specific query messages sent downstream, and use the source address of the last IGMP message received from a downstream host in report and leave messages sent upstream from the multicast router port.

Example

The following example sets the source address for proxied IGMP query messages to 10.0.1.8.

```
Console(config)#ip igmp snooping vlan 1 proxy-address 10.0.1.8
Console(config)#
```

ip igmp snooping vlan query-interval This command configures the interval between sending IGMP general queries. Use the **no** form to restore the default.

Syntax

ip igmp snooping vlan *vlan-id* query-interval *interval*

no ip igmp snooping vlan *vlan-id* query-interval

vlan-id - VLAN ID (Range: 1-4094)

interval - The interval between sending IGMP general queries. (Range: 10-31744 seconds)

Default Setting

100 (10 seconds)

Command Mode

Global Configuration

Command Usage

- ◆ An IGMP general query message is sent by the switch at the interval specified by this command. When this message is received by downstream hosts, all receivers build an IGMP report for the multicast groups they have joined.
- ◆ This command applies when the switch is serving as the querier ([page 594](#)), or as a proxy host when IGMP snooping proxy reporting is enabled ([page 594](#)).

Example

```
Console(config)#ip igmp snooping vlan 1 query-interval 150
Console(config)#
```

ip igmp snooping vlan query-resp-intvl This command configures the maximum time the system waits for a response to general queries. Use the **no** form to restore the default.

Syntax

ip igmp snooping vlan *vlan-id* query-resp-intvl *interval*

no ip igmp snooping vlan *vlan-id* query-resp-intvl

vlan-id - VLAN ID (Range: 1-4094)

interval - The maximum time the system waits for a response to general queries. (Range: 10-31740 tenths of a second)

Default Setting

100 (10 seconds)

Command Mode

Global Configuration

Command Usage

This command applies when the switch is serving as the querier ([page 594](#)), or as a proxy host when IGMP snooping proxy reporting is enabled ([page 594](#)).

Example

```
Console(config)#ip igmp snooping vlan 1 query-resp-intvl 20
Console(config)#
```

ip igmp snooping vlan static This command adds a port to a multicast group. Use the **no** form to remove the port.

Syntax

[no] ip igmp snooping vlan *vlan-id* static *ip-address* interface

vlan-id - VLAN ID (Range: 1-4094)

ip-address - IP address for multicast group

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ Static multicast entries are never aged out.
- ◆ When a multicast entry is assigned to an interface in a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

Example

The following shows how to statically configure a multicast group on a port.

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12 ethernet 1/5
Console(config)#
```

clear ip igmp snooping groups dynamic This command clears multicast group information dynamically learned through IGMP snooping.

Syntax

clear ip igmp snooping groups dynamic

Command Mode

Privileged Exec

Command Usage

This command only clears entries learned through IGMP snooping. Statically configured multicast address are not cleared.

Example

```
Console#clear ip igmp snooping groups dynamic
Console#
```

clear ip igmp snooping statistics This command clears IGMP snooping statistics.

Syntax

clear ip igmp snooping statistics [**interface** *interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

vlan *vlan-id* - VLAN identifier (Range: 1-4094)

Command Mode

Privileged Exec

Example

```
Console#clear ip igmp snooping statistics
Console#
```

show ip igmp snooping This command shows the IGMP snooping, proxy, and query configuration settings.

Syntax

show ip igmp snooping [**vlan** *vlan-id*]

vlan-id - VLAN ID (1-4094)

Command Mode
Privileged Exec**Example**

The following shows the current IGMP snooping configuration:

```

Console#show ip igmp snooping
IGMP Snooping                : Enabled
Router Port Expire Time      : 300 s
Router Alert Check           : Disabled
TCN Flood                    : Disabled
TCN Query Solicit            : Disabled
Unregistered Data Flood      : Disabled
Unsolicited Report Interval  : 400 s
Version Exclusive            : Disabled
Version                      : 2
Proxy Reporting              : Enabled
Querier                      : Disabled

VLAN 1:
-----
IGMP Snooping                : Enabled
IGMP Snooping Running Status : Inactive
Version                      : Using global version (2)
Version Exclusive            : Using global status (Disabled)
Immediate Leave              : Disabled
Last Member Query Interval   : 10 (1/10s)
Last Member Query Count      : 2
General Query Suppression    : Disabled
Query Interval               : 125
Query Response Interval      : 100 (1/10s)
Proxy Query Address          : 0.0.0.0
Proxy Reporting              : Using global status (Enabled)
Multicast Router Discovery    : Enabled
:
```

show ip igmp snooping group This command shows known multicast group, source, and host port mappings for the specified VLAN interface, or for all interfaces if none is specified.

Syntax

show ip igmp snooping group [**host-ip-addr** *ip-address* *interface* | **igmpsnp** | **sort-by-port** | **user** | **vlan** *vlan-id* [**user** | **igmpsnp**]]

ip-address - IP address for multicast group

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

igmpsnp - Display only entries learned through IGMP snooping.

sort-by-port - Display entries sorted by port.

user - Display only the user-configured multicast entries.

vlan-id - VLAN ID (1-4094)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Member types displayed include IGMP or USER, depending on selected options.

Example

The following shows the multicast entries learned through IGMP snooping for VLAN 1.

```
Console#show ip igmp snooping group vlan 1
Bridge Multicast Forwarding Entry Count:1
Flag: R - Router port, M - Group member port
      H - Host counts (number of hosts join the group on this port).
      P - Port counts (number of ports join the group).
Up time: Group elapsed time (d:h:m:s).
Expire : Group remaining time (m:s).
```

VLAN	Group	Port	Up time	Expire Count
1	224.1.1.1		00:00:00:37	2 (P)
		Eth 1/ 1 (R)		
		Eth 1/ 2 (M)		0 (H)

```
Console#
```

show ip igmp snooping mrouter This command displays information on statically configured and dynamically learned multicast router ports.

Syntax

show ip igmp snooping mrouter [**vlan** *vlan-id*]

vlan-id - VLAN ID (Range: 1-4094)

Default Setting

Displays multicast router ports for all configured VLANs.

Command Mode

Privileged Exec

Command Usage

Multicast router port types displayed include Static or Dynamic.

Example

The following shows the ports in VLAN 1 which are attached to multicast routers.

```

Console#show ip igmp snooping mrouter vlan 1
VLAN M'cast Router Port Type    Expire
-----
1    Eth 1/1                Static
Console#

```

**show ip igmp
snooping statistics**

This command shows IGMP snooping protocol statistics for the specified interface.

Syntax**show ip igmp snooping statistics**

```

{input [interface interface] |
output [interface interface] |
query [vlan vlan-id]}

```

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

vlan *vlan-id* - VLAN ID (Range: 1-4094)

query - Displays IGMP snooping-related statistics.

Default Setting

None

Command Mode

Privileged Exec

Example

The following shows IGMP protocol statistics input:

```

Console#show ip igmp snooping statistics input interface ethernet 1/1
Interface Report    Leave    G Query  G(-S)-S Query Drop    Join Succ Group
-----
Eth 1/ 1           23        11        4           10        5           14        5
Console#

```

Table 123: show ip igmp snooping statistics input - display description

Field	Description
Interface	Shows interface.
Report	The number of IGMP membership reports received on this interface.
Leave	The number of leave messages received on this interface.
G Query	The number of general query messages received on this interface.
G(-S)-S Query	The number of group specific or group-and-source specific query messages received on this interface.
Drop	The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, or packet content not allowed.
Join Succ	The number of times a multicast group was successfully joined.
Group	The number of multicast groups active on this interface.

The following shows IGMP protocol statistics output:

```

Console#show ip igmp snooping statistics output interface ethernet 1/1
Output Statistics:
Interface Report   Leave    G Query  G(-S)-S Query
-----
Eth 1/ 1          12       0        1          0
Console#

```

Table 124: show ip igmp snooping statistics output - display description

Field	Description
Interface	Shows interface.
Report	The number of IGMP membership reports sent from this interface.
Leave	The number of leave messages sent from this interface.
G Query	The number of general query messages sent from this interface.
G(-S)-S Query	The number of group specific or group-and-source specific query messages sent from this interface.

The following shows IGMP query-related statistics for VLAN 1:

```

Console#show ip igmp snooping statistics query vlan 1
Querier IP Address      : 192.168.1.1
Querier Expire Time     : 00:00:30
General Query Received  : 10
General Query Sent      : 0
Specific Query Received : 2
Specific Query Sent     : 0
Number of Reports Sent  : 2
Number of Leaves Sent   : 0
Console#

```

Table 125: show ip igmp snooping statistics vlan query - display description

Field	Description
Querier IP Address	The IP address of the querier on this interface.
Querier Expire Time	The time after which this querier is assumed to have expired.
General Query Received	The number of general queries received on this interface.
General Query Sent	The number of general queries sent from this interface.
Specific Query Received	The number of specific queries received on this interface.
Specific Query Sent	The number of specific queries sent from this interface.
Number of Reports Sent	The number of reports sent from this interface.
Number of Leaves Sent	The number of leaves sent from this interface.

Static Multicast Routing

This section describes commands used to configure static multicast routing on the switch.

Table 126: Static Multicast Interface Commands

Command	Function	Mode
<code>ip igmp snooping vlan mrouter</code>	Adds a multicast router port	GC
<code>show ip igmp snooping mrouter</code>	Shows multicast router ports	PE

ip igmp snooping vlan mrouter This command statically configures a (Layer 2) multicast router port on the specified VLAN. Use the **no** form to remove the configuration.

Syntax

[no] ip igmp snooping vlan *vlan-id* mrouter *interface*

vlan-id - VLAN ID (Range: 1-4094)

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Default Setting

No static multicast router ports are configured.

Command Mode

Global Configuration

Command Usage

- ◆ Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router or switch connected over the network to an interface (port or trunk) on this switch, that interface can be manually configured to join all the current multicast groups.
- ◆ IGMP Snooping must be enabled globally on the switch (using the [ip igmp snooping](#) command) before a multicast router port can take effect.

Example

The following shows how to configure port 10 as a multicast router port within VLAN 1.

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/10
Console(config)#
```

IGMP Filtering and Throttling

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service based on a specific subscription plan. The IGMP filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port, and IGMP throttling limits the number of simultaneous multicast groups a port can join.

Table 127: IGMP Filtering and Throttling Commands

Command	Function	Mode
ip igmp filter	Enables IGMP filtering and throttling on the switch	GC
ip igmp profile	Sets a profile number and enters IGMP filter profile configuration mode	GC
permit, deny	Sets a profile access mode to permit or deny	IPC
range	Specifies one or a range of multicast addresses for a profile	IPC
ip igmp filter	Assigns an IGMP filter profile to an interface	IC
ip igmp max-groups	Specifies an IGMP throttling number for an interface	IC
ip igmp max-groups action	Sets the IGMP throttling action for an interface	IC
ip igmp query-drop	Drops any received IGMP query packets	IC
ip multicast-data-drop	Drops all multicast data packets	IC
show ip igmp filter	Displays the IGMP filtering status	PE
show ip igmp profile	Displays IGMP profiles and settings	PE

Table 127: IGMP Filtering and Throttling Commands (Continued)

Command	Function	Mode
<code>show ip igmp query-drop</code>	Shows if the interface is configured to drop IGMP query packets	PE
<code>show ip igmp throttle interface</code>	Displays the IGMP throttling setting for interfaces	PE
<code>show ip multicast-data-drop</code>	Shows if the interface is configured to drop multicast data packets	PE

ip igmp filter (Global Configuration) This command globally enables IGMP filtering and throttling on the switch. Use the **no** form to disable the feature.

Syntax

[no] ip igmp filter

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ IGMP filtering enables you to assign a profile to a switch port that specifies multicast groups that are permitted or denied on the port. An IGMP filter profile can contain one or more, or a range of multicast addresses; but only one profile can be assigned to a port. When enabled, IGMP join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the IGMP join report is forwarded as normal. If a requested multicast group is denied, the IGMP join report is dropped.
- ◆ IGMP filtering and throttling only applies to dynamically learned multicast groups, it does not apply to statically configured groups.
- ◆ The IGMP filtering feature operates in the same manner when MVR is used to forward multicast traffic.

Example

```
Console(config)#ip igmp filter
Console(config)#
```

ip igmp profile This command creates an IGMP filter profile number and enters IGMP profile configuration mode. Use the **no** form to delete a profile number.

Syntax

[no] ip igmp profile *profile-number*

profile-number - An IGMP filter profile number. (Range: 1-4294967295)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

A profile defines the multicast groups that a subscriber is permitted or denied to join. The same profile can be applied to many interfaces, but only one profile can be assigned to one interface. Each profile has only one access mode; either permit or deny.

Example

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#
```

permit, deny This command sets the access mode for an IGMP filter profile. Use the **no** form to delete a profile number.

Syntax

{permit | deny}

Default Setting

Deny

Command Mode

IGMP Profile Configuration

Command Usage

- ◆ Each profile has only one access mode; either permit or deny.
- ◆ When the access mode is set to permit, IGMP join reports are processed when a multicast group falls within the controlled range. When the access mode is set to deny, IGMP join reports are only processed when a multicast group is not in the controlled range.

Example

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#permit
Console(config-igmp-profile)#
```

range This command specifies multicast group addresses for a profile. Use the **no** form to delete addresses from a profile.

Syntax

[no] range *low-ip-address* [*high-ip-address*]

low-ip-address - A valid IP address of a multicast group or start of a group range.

high-ip-address - A valid IP address for the end of a multicast group range.

Default Setting

None

Command Mode

IGMP Profile Configuration

Command Usage

Enter this command multiple times to specify more than one multicast address or address range for a profile.

Example

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#range 239.1.1.1
Console(config-igmp-profile)#range 239.2.3.1 239.2.3.100
Console(config-igmp-profile)#
```

ip igmp filter (Interface Configuration) This command assigns an IGMP filtering profile to an interface on the switch. Use the **no** form to remove a profile from an interface.

Syntax

[no] ip igmp filter *profile-number*

profile-number - An IGMP filter profile number. (Range: 1-4294967295)

Default Setting

None

Command Mode

Interface Configuration

Command Usage

- ◆ The IGMP filtering profile must first be created with the `ip igmp profile` command before being able to assign it to an interface.
- ◆ Only one profile can be assigned to an interface.
- ◆ A profile can also be assigned to a trunk interface. When ports are configured as trunk members, the trunk uses the filtering profile assigned to the first port member in the trunk.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp filter 19
Console(config-if)#
```

ip igmp max-groups This command sets the IGMP throttling number for an interface on the switch. Use the **no** form to restore the default setting.

Syntax

ip igmp max-groups *number*

no ip igmp max-groups

number - The maximum number of multicast groups an interface can join at the same time. (Range: 1-1024)

Default Setting

1024

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ IGMP throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either "deny" or "replace." If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.
- ◆ IGMP throttling can also be set on a trunk interface. When ports are configured as trunk members, the trunk uses the throttling settings of the first port member in the trunk.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp max-groups 10
Console(config-if)#
```

ip igmp max-groups action This command sets the IGMP throttling action for an interface on the switch.

Syntax

ip igmp max-groups action {deny | replace}

deny - The new multicast group join report is dropped.

replace - The new multicast group replaces an existing group.

Default Setting

Deny

Command Mode

Interface Configuration (Ethernet)

Command Usage

When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace.” If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp max-groups action replace
Console(config-if)#
```

ip igmp query-drop This command drops any received IGMP query packets. Use the no form to restore the default setting.

Syntax

[no] ip igmp query-drop

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

This command can be used to drop any query packets received on the specified interface. If this switch is acting as a Querier, this prevents it from being affected by messages received from another Querier.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp query-drop
Console(config-if)#
```

ip multicast-data-drop This command drops all multicast data packets

Syntax

[no] ip multicast-data-drop

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

This command can be used to stop multicast services from being forwarded to users attached to the downstream port (i.e., the interfaces specified by this command).

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip multicast-data-drop
Console(config-if)#
```

show ip igmp filter This command displays the global and interface settings for IGMP filtering.

Syntax

show ip igmp filter [**interface** *interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show ip igmp filter
IGMP filter enabled
Console#show ip igmp filter interface ethernet 1/1
Ethernet 1/1 information
-----
IGMP Profile 19
  Deny
  Range 239.1.1.1 239.1.1.1
  Range 239.2.3.1 239.2.3.100
Console#
```

show ip igmp profile This command displays IGMP filtering profiles created on the switch.

Syntax

show ip igmp profile [*profile-number*]

profile-number - An existing IGMP filter profile number.
(Range: 1-4294967295)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show ip igmp profile
IGMP Profile 19
IGMP Profile 50
Console#show ip igmp profile 19
IGMP Profile 19
  Deny
  Range 239.1.1.1 239.1.1.1
  Range 239.2.3.1 239.2.3.100
Console#
```

show ip igmp query-drop This command shows if the specified interface is configured to drop IGMP query packets.

Syntax

show ip igmp throttle interface [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Using this command without specifying an interface displays all interfaces.

Example

```
Console#show ip igmp query-drop interface ethernet 1/1
Ethernet 1/1: Enabled
Console#
```

show ip igmp throttle interface This command displays the interface settings for IGMP throttling.

Syntax

show ip igmp throttle interface [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Using this command without specifying an interface displays information for all interfaces.

Example

```
Console#show ip igmp throttle interface ethernet 1/1
Eth 1/1 Information
  Status : TRUE
  Action : Deny
  Max Multicast Groups : 32
  Current Multicast Groups : 0

Console#
```

show ip multicast-data-drop This command shows if the specified interface is configured to drop multicast data packets.

Syntax

show ip igmp throttle interface [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Using this command without specifying an interface displays all interfaces.

Example

```
Console#show ip multicast-data-drop interface ethernet 1/1
Ethernet 1/1: Enabled
Console#
```

MLD Snooping

Multicast Listener Discovery (MLD) snooping operates on IPv6 traffic and performs a similar function to IGMP snooping for IPv4. That is, MLD snooping dynamically configures switch ports to limit IPv6 multicast traffic so that it is forwarded only to ports with users that want to receive it. This reduces the flooding of IPv6 multicast packets in the specified VLANs.

There are two versions of the MLD protocol, version 1 and version 2. MLDv1 control packets include Listener Query, Listener Report, and Listener Done messages (equivalent to IGMPv2 query, report, and leave messages). MLDv2 control packets include MLDv2 query and report messages, as well as MLDv1 report and done messages.

Remember that IGMP Snooping and MLD Snooping are independent functions, and can therefore both function at the same time.

Table 128: MLD Snooping Commands

Command	Function	Mode
<code>ipv6 mld snooping</code>	Enables MLD Snooping globally	GC
<code>ipv6 mld snooping querier</code>	Allows the switch to act as the querier for MLD snooping	GC
<code>ipv6 mld snooping query-interval</code>	Configures the interval between sending MLD general query messages	GC
<code>ipv6 mld snooping query-max-response-time</code>	Configures the maximum response time for a general queries	GC
<code>ipv6 mld snooping robustness</code>	Configures the robustness variable	GC
<code>ipv6 mld snooping router-port-expire-time</code>	Configures the router port expire time	GC
<code>ipv6 mld snooping unknown-multicast mode</code>	Sets an action for unknown multicast packets	GC
<code>ipv6 mld snooping version</code>	Configures the MLD Snooping version	GC
<code>ipv6 mld snooping vlan immediate-leave</code>	Removes a member port of an IPv6 multicast service if a leave packet is received at that port and MLD immediate-leave is enabled for the parent VLAN	GC
<code>ipv6 mld snooping vlan mrouter</code>	Adds an IPv6 multicast router port	GC
<code>ipv6 mld snooping vlan static</code>	Adds an interface as a member of a multicast group	GC
<code>show ipv6 mld snooping</code>	Displays MLD Snooping configuration	PE
<code>show ipv6 mld snooping group</code>	Displays the learned groups	PE
<code>show ipv6 mld snooping group source-list</code>	Displays the learned groups and corresponding source list	PE
<code>show ipv6 mld snooping mrouter</code>	Displays the information of multicast router ports	PE

ipv6 mld snooping This command enables MLD Snooping globally on the switch. Use the **no** form to disable MLD Snooping.

Syntax

[no] ipv6 mld snooping

Default Setting

Disabled

Command Mode

Global Configuration

Example

The following example enables MLD Snooping:

```
Console(config)#ipv6 mld snooping
Console(config)#
```

ipv6 mld snooping querier This command allows the switch to act as the querier for MLDv2 snooping. Use the **no** form to disable this feature.

Syntax

[no] ipv6 mld snooping querier

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ If enabled, the switch will serve as querier if elected. The querier is responsible for asking hosts if they want to receive multicast traffic.
- ◆ An IPv6 address must be configured on the VLAN interface from which the querier will act if elected. When serving as the querier, the switch uses this IPv6 address as the query source address.
- ◆ The querier will not start or will disable itself after having started if it detects an IPv6 multicast router on the network.

Example

```
Console(config)#ipv6 mld snooping querier
Console(config)#
```

ipv6 mld snooping query-interval This command configures the interval between sending MLD general queries. Use the **no** form to restore the default.

Syntax

ipv6 mld snooping query-interval *interval*

no ipv6 mld snooping query-interval

interval - The interval between sending MLD general queries. (Range: 60-125 seconds)

Default Setting

125 seconds

Command Mode

Global Configuration

Command Usage

- ◆ This command applies when the switch is serving as the querier.
- ◆ An MLD general query message is sent by the switch at the interval specified by this command. When this message is received by downstream hosts, all receivers build an MLD report for the multicast groups they have joined.

Example

```
Console(config)#ipv6 mld snooping query-interval 150
Console(config)#
```

ipv6 mld snooping query-max-response-time This command configures the maximum response time advertised in MLD general queries. Use the **no** form to restore the default.

Syntax

ipv6 mld snooping query-max-response-time *seconds*

no ipv6 mld snooping query-max-response-time

seconds - The maximum response time allowed for MLD general queries. (Range: 5-25 seconds)

Default Setting

10 seconds

Command Mode

Global Configuration

Command Usage

This command controls how long the host has to respond to an MLD Query message before the switch deletes the group if it is the last member.

Example

```
Console(config)#ipv6 mld snooping query-max-response-time seconds 15
Console(config)#
```

ipv6 mld snooping robustness This command configures the MLD Snooping robustness variable. Use the **no** form to restore the default value.

Syntax

ipv6 mld snooping robustness *value*

no ipv6 mld snooping robustness

value - The number of the robustness variable. (Range: 2-10)

Default Setting

2

Command Mode

Global Configuration

Command Usage

A port will be removed from the receiver list for a multicast service when no MLD reports are detected in response to a number of MLD queries. The robustness variable sets the number of queries on ports for which there is no report.

Example

```
Console(config)#ipv6 mld snooping robustness 2
Console(config)#
```

ipv6 mld snooping router-port-expire-time This command configures the MLD query timeout. Use the **no** form to restore the default.

Syntax

ipv6 mld snooping router-port-expire-time *time*

no ipv6 mld snooping router-port-expire-time

time - Specifies the timeout of a dynamically learned router port.
(Range: 300-500 seconds)

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

The router port expire time is the time the switch waits after the previous querier stops before it considers the router port (i.e., the interface that had been receiving query packets) to have expired.

Example

```
Console(config)#ipv6 mld snooping router-port-expire-time 300
Console(config)#
```

ipv6 mld snooping unknown-multicast mode

This command sets the action for dealing with unknown multicast packets. Use the **no** form to restore the default.

Syntax

ipv6 mld snooping unknown-multicast mode {flood | to-router-port}

[no] ipv6 mld snooping unknown-multicast mode

flood - Floods the unknown multicast data packets to all ports.

to-router-port - Forwards the unknown multicast data packets to router ports.

Default Setting

to-router-port

Command Mode

Global Configuration

Command Usage

- ◆ When set to “flood,” any received IPv6 multicast packets that have not been requested by a host are flooded to all ports in the VLAN.
- ◆ When set to “router-port,” any received IPv6 multicast packets that have not been requested by a host are forwarded to ports that are connected to a detected multicast router.

Example

```
Console(config)#ipv6 mld snooping unknown-multicast mode flood
Console(config)#
```

ipv6 mld snooping version This command configures the MLD snooping version. Use the **no** form to restore the default.

Syntax

ipv6 mld snooping version {1 | 2}

1 - MLD version 1.

2 - MLD version 2.

Default Setting

Version 2

Command Mode

Global Configuration

Example

```
Console(config)#ipv6 mld snooping version 1
Console(config)#
```

ipv6 mld snooping vlan mrouter This command statically configures an IPv6 multicast router port. Use the **no** form to remove the configuration.

Syntax

[no] ipv6 mld snooping vlan *vlan-id* mrouter *interface*

vlan-id - VLAN ID (Range: 1-4094)

interface

ethernet *unit/port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Default Setting

No static multicast router ports are configured.

Command Mode

Global Configuration

Command Usage

Depending on your network connections, MLD snooping may not always be able to locate the MLD querier. Therefore, if the MLD querier is a known multicast router/switch connected over the network to an interface (port or trunk) on the switch, you can manually configure that interface to join all the current multicast groups.

Example

The following shows how to configure port 1 as a multicast router port within VLAN 1:

```
Console(config)#ipv6 mld snooping vlan 1 mrouter ethernet 1/1
Console(config)#
```

ipv6 mld snooping vlan static This command adds a port to an IPv6 multicast group. Use the **no** form to remove the port.

Syntax

[no] ipv6 mld snooping vlan *vlan-id* static *ipv6-address* interface

vlan - VLAN ID (Range: 1-4094)

ipv6-address - An IPv6 address of a multicast group. (Format: X:X:X:X::X)

interface

ethernet *unit/port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#ipv6 mld snooping vlan 1 static FF00:0:0:0:0:0:0:10C ethernet
1/6
Console(config)#
```

ipv6 mld snooping vlan immediate-leave This command immediately deletes a member port of an IPv6 multicast service when a leave packet is received at that port and immediate-leave is enabled for the parent VLAN. Use the **no** form to restore the default.

Syntax

[no] ipv6 mld snooping vlan *vlan-id* immediate-leave

vlan-id - A VLAN identification number. (Range: 1-4094)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ If MLD immediate-leave is *not* used, a multicast router (or querier) will send a group-specific query message when an MLD group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the specified timeout period.
- ◆ If MLD immediate-leave is enabled, the switch assumes that only one host is connected to the interface. Therefore, immediate leave should only be enabled on an interface if it is connected to only one MLD-enabled device, either a service host or a neighbor running MLD snooping.

Example

The following shows how to enable MLD immediate leave.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 mld snooping immediate-leave
Console(config-if)#
```

show ipv6 mld snooping This command shows the current MLD Snooping configuration.

Syntax

show ipv6 mld snooping

Command Mode

Privileged Exec

Example

The following shows MLD Snooping configuration information

```
Console#show ipv6 mld snooping
Service Status           : Disabled
Querier Status           : Disabled
Robustness                : 2
Query Interval           : 125 sec
Query Max Response Time  : 10 sec
Router Port Expiry Time  : 300 sec
Immediate Leave          : Disabled on all VLAN
Unknown Flood Behavior    : To Router Port
MLD Snooping Version     : Version 2
Console#
```

show ipv6 mld snooping group This command shows known multicast groups, member ports, and the means by which each group was learned.

Syntax

show ipv6 mld snooping group

Command Mode

Privileged Exec

Example

The following shows MLD Snooping group configuration information:

```
Console#show ipv6 mld snooping group

VLAN Multicast IPv6 Address      Member port Type
-----
  1 FF02::01:01:01:01           Eth 1/1      MLD Snooping
  1 FF02::01:01:01:02           Eth 1/1      Multicast Data
  1 FF02::01:01:01:02           Eth 1/1      User

Console#
```

show ipv6 mld snooping group source-list This command shows known multicast groups, member ports, the means by which each group was learned, and the corresponding source list.

Syntax

show ipv6 mld snooping group source-list

Command Mode

Privileged Exec

Example

The following shows MLD Snooping group mapping information:

```
Console#show ipv6 mld snooping group source-list

Console#show ipv6 mld snooping group source-list
VLAN ID                : 1
Multicast IPv6 Address  : FF02::01:01:01:01
Member Port             : Eth 1/1
Type                   : MLD Snooping
Filter Mode             : Include
(if exclude filter mode)
Filter Timer elapse     : 10 sec.
Request List            : ::01:02:03:04, ::01:02:03:05, ::01:02:03:06,
                        : ::01:02:03:07
Exclude List            : ::02:02:03:04, ::02:02:03:05, ::02:02:03:06,
                        : ::02:02:03:07
(if include filter mode)
Include List            : ::02:02:03:04, ::02:02:03:05, ::02:02:03:06,
                        : ::02:02:03:06
```



```
Option:
  Filter Mode: Include, Exclude

Console#
```

show ipv6 mld snooping mrouter

This command shows MLD Snooping multicast router information.

Syntax

show ipv6 mld snooping mrouter vlan *vlan-id*

vlan-id - A VLAN identification number. (Range: 1-4094)

Command Mode

Privileged Exec

Example

```
Console#show ipv6 mld snooping mrouter vlan 1
VLAN Multicast Router Port Type      Expire
-----
  1 Eth 1/ 2              Static

Console#
```

MVR for IPv4

This section describes commands used to configure Multicast VLAN Registration for IPv4 (MVR). A single network-wide VLAN can be used to transmit multicast traffic (such as television channels) across a service provider's network. Any multicast traffic entering an MVR VLAN is sent to all subscribers. This can significantly reduce to processing overhead required to dynamically monitor and establish the distribution tree for a normal multicast VLAN. Also note that MVR maintains the user isolation and data security provided by VLAN segregation by passing only multicast traffic into other VLANs to which the subscribers belong.

Table 129: Multicast VLAN Registration for IPv4 Commands

Command	Function	Mode
<code>mvr</code>	Globally enables MVR	GC
<code>mvr associated-profile</code>	Binds the MVR group addresses specified in a profile to an MVR domain	GC
<code>mvr domain</code>	Enables MVR for a specific domain	GC
<code>mvr profile</code>	Maps a range of MVR group addresses to a profile	GC
<code>mvr proxy-query-interval</code>	Configures the interval at which the receiver port sends out general queries.	GC

Table 129: Multicast VLAN Registration for IPv4 Commands (Continued)

Command	Function	Mode
<code>mvr proxy-switching</code>	Enables MVR proxy switching, where the source port acts as a host, and the receiver port acts as an MVR router with querier service enabled	GC
<code>mvr robustness-value</code>	Configures the expected packet loss, and thereby the number of times to generate report and group-specific queries	GC
<code>mvr source-port-mode dynamic</code>	Configures the switch to only forward multicast streams which the source port has dynamically joined	GC
<code>mvr upstream-source-ip</code>	Configures the source IP address assigned to all control packets sent upstream	GC
<code>mvr vlan</code>	Specifies the VLAN through which MVR multicast data is received	GC
<code>mvr immediate-leave</code>	Enables immediate leave capability	IC
<code>mvr type</code>	Configures an interface as an MVR receiver or source port	IC
<code>mvr vlan group</code>	Statically binds a multicast group to a port	IC
<code>clear mvr groups dynamic</code>	Clears multicast group information dynamically learned through MVR	PE
<code>clear mvr statistics</code>	Clears MVR statistics	PE
<code>show mvr</code>	Shows information about MVR domain settings, including MVR operational status, the multicast VLAN, the current number of group addresses, and the upstream source IP address	PE
<code>show mvr associated-profile</code>	Shows the profiles bound the specified domain	PE
<code>show mvr interface</code>	Shows MVR settings for interfaces attached to the MVR VLAN	PE
<code>show mvr members</code>	Shows information about the current number of entries in the forwarding database, or detailed information about a specific multicast address	PE
<code>show mvr profile</code>	Shows all configured MVR profiles	PE
<code>show mvr statistics</code>	Shows MVR protocol statistics for the specified interface	PE

mvr This command enables Multicast VLAN Registration (MVR) globally on the switch. Use the **no** form of this command to globally disable MVR.

Syntax

[no] mvr

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

Only IGMP version 2 or 3 hosts can issue multicast join or leave messages. If MVR must be configured for an IGMP version 1 host, the multicast groups must be statically assigned using the **mvr vlan group** command.

Example

The following example enables MVR globally.

```
Console(config)#mvr
Console(config)#
```

mvr associated-profile This command binds the MVR group addresses specified in a profile to an MVR domain. Use the **no** form of this command to remove the binding.

Syntax

[no] mvr domain *domain-id* associated-profile *profile-name*

domain-id - An independent multicast domain. (Range: 1-5)

profile-name - The name of a profile containing one or more MVR group addresses. (Range: 1-21 characters)

Default Setting

Disabled

Command Mode

Global Configuration

Example

The following an MVR group address profile to domain 1:

```
Console(config)#mvr domain 1 associated-profile rd
Console(config)#
```

Related Commands

[mvr profile \(636\)](#)

mvr domain This command enables Multicast VLAN Registration (MVR) for a specific domain. Use the **no** form of this command to disable MVR for a domain.

Syntax

[no] mvr domain *domain-id*

domain-id - An independent multicast domain. (Range: 1-5)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

Only IGMP version 2 or 3 hosts can issue multicast join or leave messages. If MVR must be configured for an IGMP version 1 host, the multicast groups must be statically assigned using the [mvr vlan group](#) command.

Example

The following example enables MVR for domain 1:

```
Console(config)#mvr domain 1
Console(config)#
```

mvr profile This command maps a range of MVR group addresses to a profile. Use the **no** form of this command to remove the profile.

Syntax

mvr profile *profile-name start-ip-address end-ip-address*

profile-name - The name of a profile containing one or more MVR group addresses. (Range: 1-21 characters)

start-ip-address - Starting IPv4 address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)

end-ip-address - Ending IPv4 address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)

Default Setting

No profiles are defined

Command Mode

Global Configuration

Command Usage

- ◆ Use this command to statically configure all multicast group addresses that will join the MVR VLAN. Any multicast data associated an MVR group is sent from all source ports to all receiver ports that have registered to receive data from that multicast group.
- ◆ The IP address range from 224.0.0.0 to 239.255.255.255 is used for multicast streams. MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x.
- ◆ IGMP snooping and MVR share a maximum number of 1024 groups. Any multicast streams received in excess of this limitation will be flooded to all ports in the associated domain.

Example

The following example maps a range of MVR group addresses to a profile:

```
Console(config)#mvr profile rd 228.1.23.1 228.1.23.10  
Console(config)#
```

mvr proxy-query-interval This command configures the interval at which the receiver port sends out general queries. Use the **no** form to restore the default setting.

Syntax

mvr proxy-query-interval *interval*

no mvr proxy-query-interval

interval - The interval at which the receiver port sends out general queries.
(Range: 2-31744 seconds)

Default Setting

125 seconds

Command Mode

Global Configuration

Command Usage

This command sets the general query interval at which active receiver ports send out general queries. This interval is only effective when proxy switching is enabled with the [mvr proxy-switching](#) command.

Example

This example sets the proxy query interval for MVR proxy switching.

```
Console(config)#mvr proxy-query-interval 250  
Console(config)#
```

mvr proxy-switching This command enables MVR proxy switching, where the source port acts as a host, and the receiver port acts as an MVR router with querier service enabled. Use the **no** form to disable this function.

Syntax

[no] mvr proxy-switching

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

- ◆ When MVR proxy-switching is enabled, an MVR source port serves as the upstream or host interface. The source port performs only the host portion of MVR by sending summarized membership reports, and automatically disables MVR router functions.
- ◆ Receiver ports are known as downstream or router interfaces. These interfaces perform the standard MVR router functions by maintaining a database of all MVR subscriptions on the downstream interface. Receiver ports must therefore be configured on all downstream interfaces which require MVR proxy service.
- ◆ When the source port receives report and leave messages, it only forwards them to other source ports.
- ◆ When receiver ports receive any query messages, they are dropped.
- ◆ When changes occurring in the downstream MVR groups are learned by the receiver ports through report and leave messages, an MVR state change report is created and sent to the upstream source port, which in turn forwards this information upstream.
- ◆ When MVR proxy switching is disabled:
 - Any membership reports received from receiver/source ports are forwarded to all source ports.
 - When a source port receives a query message, it will be forwarded to all downstream receiver ports.
 - When a receiver port receives a query message, it will be dropped.

Example

The following example enable MVR proxy switching.

```
Console(config)#mvr proxy-switching
Console(config)#
```

Related Commands

[mvr robustness-value \(639\)](#)

mvr robustness-value This command configures the expected packet loss, and thereby the number of times to generate report and group-specific queries. Use the **no** form to restore the default setting.

Syntax

mvr robustness-value *value*

no mvr robustness-value

value - The robustness used for all interfaces. (Range: 1-255)

Default Setting

2

Command Mode

Global Configuration

Command Usage

- ◆ This command is used to set the number of times report messages are sent upstream when changes are learned about downstream groups, and the number of times group-specific queries are sent to downstream receiver ports.
- ◆ This command only takes effect when MVR proxy switching is enabled.

Example

```
Console(config)#mvr robustness-value 5
Console(config)#
```

Related Commands

[mvr proxy-switching \(638\)](#)

mvr source-port-mode dynamic This command configures the switch to only forward multicast streams which the source port has dynamically joined. Use the **no** form to restore the default setting.

Syntax

[no] mvr source-port-mode dynamic

Default Setting

Forwards all multicast streams which have been specified in a profile and bound to a domain.

Command Mode

Global Configuration

Command Usage

- ◆ By default, the switch forwards any multicast streams within the address range set by a profile, and bound to a domain. The multicast streams are sent to all source ports on the switch and to all receiver ports that have elected to receive data on that multicast address.
- ◆ When the **mvr source-port-mode dynamic** command is used, the switch only forwards multicast streams which the source port has dynamically joined. In other words, both the receiver port and source port must subscribe to a multicast group before a multicast stream is forwarded to any attached client. Note that the requested streams are still restricted to the address range which has been specified in a profile and bound to a domain.

Example

```
Console(config)#mvr source-port-mode dynamic
Console(config)#
```

mvr upstream-source-ip This command configures the source IP address assigned to all MVR control packets sent upstream on all domains or on a specified domain. Use the **no** form to restore the default setting.

Syntax

mvr [domain *domain-id*] upstream-source-ip *source-ip-address*

no mvr [domain *domain-id*] upstream-source-ip

domain-id - An independent multicast domain. (Range: 1-5)

source-ip-address – The source IPv4 address assigned to all MVR control packets sent upstream.

Default Setting

All MVR reports sent upstream use a null source IP address

Command Mode

Global Configuration

Example

```
Console(config)#mvr domain 1 upstream-source-ip 192.168.0.3
Console(config)#
```

mvr vlan This command specifies the VLAN through which MVR multicast data is received. Use the **no** form of this command to restore the default MVR VLAN.

Syntax

mvr domain *domain-id* **vlan** *vlan-id*

no mvr domain *domain-id* **vlan**

domain-id - An independent multicast domain. (Range: 1-5)

vlan-id - Specifies the VLAN through which MVR multicast data is received. This is also the VLAN to which all source ports must be assigned. (Range: 1-4094)

Default Setting

VLAN 1

Command Mode

Global Configuration

Command Usage

- ◆ This command specifies the VLAN through which MVR multicast data is received. This is the VLAN to which all source ports must be assigned.
- ◆ The VLAN specified by this command must be an existing VLAN configured with the **vlan** command.
- ◆ MVR source ports can be configured as members of the MVR VLAN using the **switchport allowed vlan** command and **switchport native vlan** command, but MVR receiver ports should not be statically configured as members of this VLAN.

Example

The following example sets the MVR VLAN to VLAN 2:

```
Console(config)#mvr
Console(config)#mvr domain 1 vlan 2
Console(config)#
```

mvr immediate-leave This command causes the switch to immediately remove an interface from a multicast stream as soon as it receives a leave message for that group. Use the **no** form to restore the default settings.

Syntax

[no] mvr [domain *domain-id*] immediate-leave

domain-id - An independent multicast domain. (Range: 1-5)

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ Immediate leave applies only to receiver ports. When enabled, the receiver port is immediately removed from the multicast group identified in the leave message. When immediate leave is disabled, the switch follows the standard rules by sending a group-specific query to the receiver port and waiting for a response to determine if there are any remaining subscribers for that multicast group before removing the port from the group list.
- ◆ Using immediate leave can speed up leave latency, but should only be enabled on a port attached to only one multicast subscriber to avoid disrupting services to other group members attached to the same interface.
- ◆ Immediate leave does not apply to multicast groups which have been statically assigned to a port with the [mvr vlan group](#) command.

Example

The following enables immediate leave on a receiver port.

```
Console(config)#interface ethernet 1/5
Console(config-if)#mvr domain 1 immediate-leave
Console(config-if)#
```

mvr type This command configures an interface as an MVR receiver or source port. Use the **no** form to restore the default settings.

Syntax

[no] **mvr** [domain *domain-id*] **type** {**receiver** | **source**}

domain-id - An independent multicast domain. (Range: 1-5)

receiver - Configures the interface as a subscriber port that can receive multicast data.

source - Configures the interface as an uplink port that can send and receive multicast data for the configured multicast groups.

Default Setting

The port type is not defined.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ A port which is not configured as an MVR receiver or source port can use IGMP snooping to join or leave multicast groups using the standard rules for multicast filtering.
- ◆ Receiver ports can belong to different VLANs, but should not normally be configured as a member of the MVR VLAN. IGMP snooping can also be used to allow a receiver port to dynamically join or leave multicast groups not sourced through the MVR VLAN.
- ◆ One or more interfaces may be configured as MVR source ports. A source port is able to both receive and send data for multicast groups which it has joined through the MVR protocol or which have been assigned through the **mvr vlan group** command.
- ◆ Only IGMP version 2 or 3 hosts can issue multicast join or leave messages. If MVR must be configured for an IGMP version 1 host, the multicast groups must be statically assigned using the **mvr vlan group** command.

Example

The following configures one source port and several receiver ports on the switch.

```
Console(config)#interface ethernet 1/5
Console(config-if)#mvr domain 1 type source
Console(config-if)#exit
Console(config)#interface ethernet 1/6
Console(config-if)#mvr domain 1 type receiver
Console(config-if)#exit
Console(config)#interface ethernet 1/7
Console(config-if)#mvr domain 1 type receiver
Console(config-if)#
```

mvr vlan group This command statically binds a multicast group to a port which will receive long-term multicast streams associated with a stable set of hosts. Use the **no** form to restore the default settings.

Syntax

[no] mvr [domain *domain-id*] vlan *vlan-id* group *ip-address*

domain-id - An independent multicast domain. (Range: 1-5)

vlan-id - Receiver VLAN to which the specified multicast traffic is flooded.
(Range: 1-4094)

group - Defines a multicast service sent to the selected port.

ip-address - Statically configures an interface to receive multicast traffic from the IPv4 address specified for an MVR multicast group.
(Range: 224.0.1.0 - 239.255.255.255)

Default Setting

No receiver port is a member of any configured multicast group.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ Multicast groups can be statically assigned to a receiver port using this command.
- ◆ The IP address range from 224.0.0.0 to 239.255.255.255 is used for multicast streams. MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x.
- ◆ Only IGMP version 2 or 3 hosts can issue multicast join or leave messages. If MVR must be configured for an IGMP version 1 host, the multicast groups must be statically assigned using the **mvr vlan group** command.
- ◆ The MVR VLAN cannot be specified as the receiver VLAN for static bindings.

Example

The following statically assigns a multicast group to a receiver port:

```
Console(config)#interface ethernet 1/7
Console(config-if)#mvr domain 1 type receiver
Console(config-if)#mvr domain 1 vlan 3 group 225.0.0.5
Console(config-if)#
```

clear mvr groups dynamic This command clears multicast group information dynamically learned through MVR.

Syntax

clear mvr groups dynamic

Command Mode

Privileged Exec

Command Usage

This command only clears entries learned through MVR. Statically configured multicast addresses are not cleared.

Example

```
Console#clear mvr groups r&d
Console#
```

clear mvr statistics This command clears MVR statistics.

Syntax

clear mvr statistics [**interface** *interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

vlan *vlan-id* - VLAN identifier (Range: 1-4094)

Command Mode

Privileged Exec

Example

```
Console#clear mvr statistics
Console#
```

show mvr This command shows information about MVR domain settings, including MVR operational status, the multicast VLAN, the current number of group addresses, and the upstream source IP address.

Syntax

show mvr [**domain** *domain-id*]

domain-id - An independent multicast domain. (Range: 1-5)

Default Setting

Displays configuration settings for all MVR domains.

Command Mode

Privileged Exec

Example

The following shows the MVR settings:

```
Console#show mvr
MVR Proxy Switching           : Enabled
MVR Robustness Value          : 1
MVR Proxy Query Interval      : 125(sec.)
MVR Source Port Mode          : Always Forward

MVR Domain                    : 1
MVR Config Status             : Enabled
MVR Running Status            : Active
MVR Multicast VLAN            : 1
MVR Current Learned Groups    : 10
MVR Upstream Source IP        : 192.168.0.3
:
```

Table 130: show mvr - display description

Field	Description
MVR Proxy Switching	Shows if MVR proxy switching is enabled
MVR Robustness Value	Shows the number of reports or query messages sent when proxy switching is enabled
MVR Proxy Query Interval	Shows the interval at which the receiver port sends out general queries
MVR Source Port Mode	Shows if the switch forwards all multicast streams, or only those which the source port has dynamically joined
MVR Domain	An independent multicast domain.
MVR Config Status	Shows if MVR is globally enabled on the switch.
MVR Running Status	Indicates whether or not all necessary conditions in the MVR environment are satisfied. (Running status is true as long as MVR Status is enabled, and the specified MVR VLAN exists.)
MVR Multicast VLAN	Shows the VLAN used to transport all MVR multicast traffic.

Table 130: show mvr - display description (Continued)

Field	Description
MVR Current Learned Groups	The current number of MVR group addresses
MVR Upstream Source IP	The source IP address assigned to all upstream control packets.

show mvr associated-profile This command shows the profiles bound the specified domain.

Syntax

show mvr [domain *domain-id*] associated-profile

domain-id - An independent multicast domain. (Range: 1-5)

Default Setting

Displays profiles bound to all MVR domains.

Command Mode

Privileged Exec

Example

The following displays the profiles bound to domain 1:

```

Console#show mvr domain 1 associated-profile
Domain ID : 1
MVR Profile Name      Start IP Addr.  End IP Addr.
-----
rd                    228.1.23.1    228.1.23.10
testing               228.2.23.1    228.2.23.10
Console#

```

show mvr interface This command shows MVR configuration settings for interfaces attached to the MVR VLAN.

Syntax

show mvr [domain *domain-id*] interface

domain-id - An independent multicast domain. (Range: 1-5)

Default Setting

Displays configuration settings for all attached interfaces.

Command Mode

Privileged Exec

Example

The following displays information about the interfaces attached to the MVR VLAN in domain 1:

```
Console#show mvr domain 1 interface
MVR Domain : 1
Port          Type          Status          Immediate      Static Group Address
-----
Eth 1/ 1 Source    Active/Forwarding
Eth 1/ 2 Receiver Inactive/Discarding Disabled      234.5.6.8 (VLAN2)
Eth1/ 3 Source    Inactive/Discarding
Eth1/ 1 Receiver Active/Forwarding Disabled      225.0.0.1 (VLAN1)
                                           225.0.0.9 (VLAN3)
Eth1/ 4 Receiver Active/Discarding Disabled
Console#
```

Table 131: show mvr interface - display description

Field	Description
MVR Domain	An independent multicast domain.
Port	Shows interfaces attached to the MVR.
Type	Shows the MVR port type.
Status	Shows the MVR status and interface status. MVR status for source ports is "ACTIVE" if MVR is globally enabled on the switch. MVR status for receiver ports is "ACTIVE" only if there are subscribers receiving multicast traffic from one of the MVR groups, or a multicast group has been statically assigned to an interface. Also shows if MVR traffic is being forwarded or discarded.
Immediate	Shows if immediate leave is enabled or disabled.
Static Group Address	Shows any static MVR group assigned to an interface, and the receiver VLAN.

show mvr members This command shows information about the current number of entries in the forwarding database, detailed information about a specific multicast address, the IP address of the hosts subscribing to all active multicast groups, or the multicast groups associated with each port.

Syntax

show mvr [**domain** *domain-id*] **members** [*ip-address* |
host-ip-address [*interface*] | **sort-by-port** [*interface*]]

domain-id - An independent multicast domain. (Range: 1-5)

ip-address - IPv4 address for an MVR multicast group.
(Range: 224.0.1.0 - 239.255.255.255)

members - The multicast groups assigned to the MVR VLAN.

host-ip-address - The subscriber IP addresses.

sort-by-port - The multicast groups associated with an interface.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Default Setting

Displays configuration settings for all domains and all forwarding entries.

Command Mode

Privileged Exec

Example

The following shows information about the number of multicast forwarding entries currently active in domain 1:

```
Console#show mvr domain 1 members
MVR Domain : 1
MVR Forwarding Entry Count :1
Flag: S - Source port, R - Receiver port.
      H - Host counts (number of hosts joined to group on this port).
      P - Port counts (number of ports joined to group).
Up time: Group elapsed time (d:h:m:s).
Expire : Group remaining time (m:s).

Group Address  VLAN Port      Up time      Expire Count
-----
234.5.6.7      1              00:00:09:17      2 (P)
                1 Eth 1/ 1 (S)
                2 Eth 1/ 2 (R)
```

Console#

The following example shows detailed information about a specific multicast address:

```
Console#show mvr domain 1 members 234.5.6.7
MVR Domain : 1
MVR Forwarding Entry Count :1
Flag: S - Source port, R - Receiver port.
      H - Host counts (number of hosts joined to group on this port).
      P - Port counts (number of ports joined to group).
Up time: Group elapsed time (d:h:m:s).
Expire : Group remaining time (m:s).

Group Address  VLAN Port      Up time      Expire Count
-----
234.5.6.7      1              00:00:09:17      2 (P)
                1 Eth 1/ 1 (S)
                2 Eth 1/ 2 (R)
```

Console#

Table 132: show mvr members - display description

Field	Description
Group Address	Multicast group address.
VLAN	VLAN to which this address is forwarded.
Port	Port to which this address is forwarded.
Uptime	Time that this multicast group has been known.
Expire	The time until this entry expires.
Count	The number of times this address has been learned by IGMP snooping.

show mvr profile This command shows all configured MVR profiles.

Command Mode
Privileged Exec

Example

The following shows all configured MVR profiles:

```
Console#show mvr profile
MVR Profile Name      Start IP Addr.  End IP Addr.
-----
rd                    228.1.23.1     228.1.23.10
testing               228.2.23.1     228.2.23.10
Console#
```

show mvr statistics This command shows MVR protocol-related statistics for the specified interface.

Syntax

show mvr statistics {input | output} [interface *interface*]

show mvr domain *domain-id* **statistics**

{input [interface *interface*] | output [interface *interface*] | query}

domain-id - An independent multicast domain. (Range: 1-5)

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

vlan *vlan-id* - VLAN ID (Range: 1-4094)

query - Displays MVR query-related statistics.

Default Setting

Displays statistics for all domains.

Command Mode

Privileged Exec

Example

The following shows MVR protocol-related statistics received:

```

Console#show mvr domain 1 statistics input
MVR Domain : 1
Input Statistics:
Interface Report    Leave    G Query  G(-S)-S Query Drop    Join Succ Group
-----
Eth 1/ 1           23       11        4          10        5        20        9
Eth 1/ 2           12       15        8           3        5        19        4
VLAN    1           2        0         0           2        2        20        9
Console#

```

Table 133: show mvr statistics input - display description

Field	Description
Interface	Shows interfaces attached to the MVR.
Report	The number of IGMP membership reports received on this interface.
Leave	The number of leave messages received on this interface.
G Query	The number of general query messages received on this interface.
G(-S)-S Query	The number of group specific or group-and-source specific query messages received on this interface.
Drop	The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR group report received
Join Succ	The number of times a multicast group was successfully joined.
Group	The number of MVR groups active on this interface.

The following shows MVR protocol-related statistics sent:

```

Console#show mvr domain 1 statistics output
MVR Domain : 1
Output Statistics:
Interface Report    Leave    G Query  G(-S)-S Query
-----
Eth 1/ 1           12        0         1           0
Eth 1/ 2           5         1         4           1
VLAN    1           7         2         3           0
Console#

```

Table 134: show mvr statistics output - display description

Field	Description
Interface	Shows interfaces attached to the MVR.
Report	The number of IGMP membership reports sent from this interface.
Leave	The number of leave messages sent from this interface.
G Query	The number of general query messages sent from this interface.
G(-S)-S Query	The number of group specific or group-and-source specific query messages sent from this interface.

The following shows MVR query-related statistics:

```
Console#show mvr domain 1 statistics query
Querier IP Address      : 192.168.1.1
Querier Expire Time     : 00:00:30
General Query Received  : 10
General Query Sent      : 0
Specific Query Received : 2
Specific Query Sent     : 0
Number of Reports Sent  : 2
Number of Leaves Sent   : 0
Console#
```

Table 135: show mvr statistics query - display description

Field	Description
Querier IP Address	The IP address of the querier on this interface.
Querier Expire Time	The time after which this querier is assumed to have expired.
General Query Received	The number of general queries received on this interface.
General Query Sent	The number of general queries sent from this interface.
Specific Query Received	The number of specific queries received on this interface.
Specific Query Sent	The number of specific queries sent from this interface.
Number of Reports Sent	The number of reports sent from this interface.
Number of Leaves Sent	The number of leaves sent from this interface.

MVR for IPv6

This section describes commands used to configure Multicast VLAN Registration for IPv6 (MVR6). A single network-wide VLAN can be used to transmit multicast traffic (such as television channels) across a service provider's network. Any multicast traffic entering an MVR VLAN is sent to all subscribers. This can significantly reduce to processing overhead required to dynamically monitor and establish the distribution tree for a normal multicast VLAN. Also note that MVR maintains the user isolation and data security provided by VLAN segregation by passing only multicast traffic into other VLANs to which the subscribers belong.

Table 136: Multicast VLAN Registration for IPv6 Commands

Command	Function	Mode
<code>mvr6 associated-profile</code>	Binds the MVR group addresses specified in a profile to an MVR domain	GC
<code>mvr6 domain</code>	Enables MVR for a specific domain	GC
<code>mvr6 profile</code>	Maps a range of MVR group addresses to a profile	GC
<code>mvr6 proxy-query-interval</code>	Configures the interval at which the receiver port sends out general queries.	GC
<code>mvr6 proxy-switching</code>	Enables MVR proxy switching, where the source port acts as a host, and the receiver port acts as an MVR router with querier service enabled	GC
<code>mvr6 robustness-value</code>	Configures the expected packet loss, and thereby the number of times to generate report and group-specific queries	GC
<code>mvr6 source-port-mode dynamic</code>	Configures the switch to only forward multicast streams which the source port has dynamically joined	GC
<code>mvr6 upstream-source-ip</code>	Configures the source IP address assigned to all control packets sent upstream	GC
<code>mvr6 vlan</code>	Specifies the VLAN through which MVR multicast data is received	GC
<code>mvr6 immediate-leave</code>	Enables immediate leave capability	IC
<code>mvr6 type</code>	Configures an interface as an MVR receiver or source port	IC
<code>mvr6 vlan group</code>	Statically binds a multicast group to a port	IC
<code>clear mvr6 groups dynamic</code>	Clears multicast group information dynamically learned through MVR	PE
<code>clear mvr6 statistics</code>	Clears MVR statistics	PE
<code>show mvr6</code>	Shows information about MVR domain settings, including MVR operational status, the multicast VLAN, the current number of group addresses, and the upstream source IP address	PE
<code>show mvr6 associated-profile</code>	Shows the profiles bound the specified domain	PE
<code>show mvr6 interface</code>	Shows MVR settings for interfaces attached to the MVR VLAN	PE

Table 136: Multicast VLAN Registration for IPv6 Commands (Continued)

Command	Function	Mode
<code>show mvr6 members</code>	Shows information about the current number of entries in the forwarding database, or detailed information about a specific multicast address	PE
<code>show mvr6 profile</code>	Shows all configured MVR profiles	PE
<code>show mvr6 statistics</code>	Shows MVR protocol statistics for the specified interface	PE

mvr6 associated-profile This command binds the MVR group addresses specified in a profile to an MVR domain. Use the **no** form of this command to remove the binding.

Syntax

[no] mvr6 domain *domain-id* **associated-profile** *profile-name*

domain-id - An independent multicast domain. (Range: 1-5)

profile-name - The name of a profile containing one or more MVR group addresses. (Range: 1-21 characters)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

MVR6 domains can be associated with more than one MVR6 profile. But since MVR6 domains cannot share the group range, an MVR6 profile can only be associated with one MVR6 domain.

Example

The following an MVR group address profile to domain 1:

```
Console(config)#mvr6 domain 1 associated-profile rd
Console(config)#
```

mvr6 domain This command enables Multicast VLAN Registration (MVR) for a specific domain. Use the **no** form of this command to disable MVR for a domain.

Syntax

[no] mvr6 domain *domain-id*

domain-id - An independent multicast domain. (Range: 1-5)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

When MVR6 is enabled on a domain, any multicast data associated with an MVR6 group is sent from all designated source ports, to all receiver ports that have registered to receive data from that multicast group.

Example

The following example enables MVR for domain 1:

```
Console(config)#mvr6 domain 1
Console(config)#
```

mvr6 profile This command maps a range of MVR group addresses to a profile. Use the **no** form of this command to remove the profile.

Syntax

mvr6 profile *profile-name start-ip-address end-ip-address*

profile-name - The name of a profile containing one or more MVR group addresses. (Range: 1-21 characters)

start-ip-address - Starting IPv6 address for an MVR multicast group. This parameter must be a full IPv6 address including the network prefix and host address bits.

end-ip-address - Ending IPv6 address for an MVR multicast group. This parameter must be a full IPv6 address including the network prefix and host address bits.

Default Setting

No profiles are defined

Command Mode

Global Configuration

Command Usage

- ◆ Use this command to statically configure all multicast group addresses that will join the MVR VLAN. Any multicast data associated with an MVR group is sent from all source ports, and to all receiver ports that have registered to receive data from that multicast group.
- ◆ All IPv6 addresses must be according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double

colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. (Note that the IP address ff02::X is reserved.)

- ◆ The MVR6 group address range assigned to a profile cannot overlap with the group address range of any other profile.

Example

The following example maps a range of MVR group addresses to a profile:

```
Console(config)#mvr6 profile rd ff00::1 ff00::9
Console(config)#
```

mvr6 proxy-query-interval This command configures the interval at which the receiver port sends out general queries. Use the **no** form to restore the default setting.

Syntax

mvr proxy-query-interval *interval*

no mvr proxy-query-interval

interval - The interval at which the receiver port sends out general queries.
(Range: 2-31744 seconds)

Default Setting

125 seconds

Command Mode

Global Configuration

Command Usage

This command sets the general query interval at which active receiver ports send out general queries. This interval is only effective when proxy switching is enabled with the [mvr6 proxy-switching](#) command.

Example

This example sets the proxy query interval for MVR proxy switching.

```
Console(config)#mvr profile rd 228.1.23.1 228.1.23.10
Console(config)#
```


mvr6 proxy-switching This command enables MVR proxy switching, where the source port acts as a host, and the receiver port acts as an MVR router with querier service enabled. Use the **no** form to disable this function.

Syntax

[no] mvr6 proxy-switching

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

- ◆ When MVR proxy-switching is enabled, an MVR source port serves as the upstream or host interface, and the MVR receiver port serves as the querier. The source port performs only the host portion of MVR by sending summarized membership reports, and automatically disables MVR router functions.
- ◆ Receiver ports are known as downstream or router interfaces. These interfaces perform the standard MVR router functions by maintaining a database of all MVR subscriptions on the downstream interface. Receiver ports must therefore be configured on all downstream interfaces which require MVR proxy service.
- ◆ When the source port receives report and leave messages, it only forwards them to other source ports.
- ◆ When receiver ports receive any query messages, they are dropped.
- ◆ When changes occurring in the downstream MVR groups are learned by the receiver ports through report and leave messages, an MVR state change report is created and sent to the upstream source port, which in turn forwards this information upstream.
- ◆ When MVR proxy switching is disabled:
 - Any membership reports received from receiver/source ports are forwarded to all source ports.
 - When a source port receives a query message, it will be forwarded to all downstream receiver ports.
 - When a receiver port receives a query message, it will be dropped.

Example

The following example enable MVR proxy switching.

```
Console(config)#mvr proxy-switching
Console(config)#
```

Related Commands

[mvr6 robustness-value \(658\)](#)

mvr6 robustness-value This command configures the expected packet loss, and thereby the number of times to generate report and group-specific queries. Use the **no** form to restore the default setting.

Syntax

mvr6 robustness-value *value*

no mvr6 robustness-value

value - The robustness used for all interfaces. (Range: 1-10)

Default Setting

1

Command Mode

Global Configuration

Command Usage

- ◆ This command is used to set the number of times report messages are sent upstream when changes are learned about downstream groups, and the number of times group-specific queries are sent to downstream receiver ports.
- ◆ This command only takes effect when MVR6 proxy switching is enabled.

Example

```
Console(config)#mvr6 robustness-value 5
Console(config)#
```

Related Commands

[mvr6 proxy-switching \(657\)](#)

mvr6 source-port-mode dynamic This command configures the switch to only forward multicast streams which the source port has dynamically joined. Use the **no** form to restore the default setting.

Syntax

[no] **mvr6 source-port-mode dynamic**

Default Setting

Forwards all multicast streams which have been specified in a profile and bound to a domain.

Command Mode

Global Configuration

Command Usage

- ◆ By default, the switch forwards any multicast streams within the address range set by a profile, and bound to a domain. The multicast streams are sent to all source ports on the switch and to all receiver ports that have elected to receive data on that multicast address.
- ◆ When the **mvr6 source-port-mode dynamic** command is used, the switch only forwards multicast streams which the source port has dynamically joined. In other words, both the receiver port and source port must subscribe to a multicast group before a multicast stream is forwarded to any attached client. Note that the requested streams are still restricted to the address range which has been specified in a profile and bound to a domain.

Example

```
Console(config)#mvr6 source-port-mode dynamic
Console(config)#
```

mvr6 upstream-source-ip This command configures the source IPv6 address assigned to all MVR control packets sent upstream on the specified domain. Use the **no** form to restore the default setting.

Syntax

mvr6 domain *domain-id* **upstream-source-ip** *source-ip-address*

no mvr6 domain *domain-id* **upstream-source-ip**

domain-id - An independent multicast domain. (Range: 1-5)

source-ip-address – The source IPv6 address assigned to all MVR control packets sent upstream. This parameter must be a full IPv6 address including the network prefix and host address bits.

Default Setting

All MVR reports sent upstream use a null source IP address

Command Mode

Global Configuration

Command Usage

All IPv6 addresses must be according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. (Note that the IP address ff02::X is reserved.)

Example

```
Console(config)#mvr6 domain 1 upstream-source-ip 2001:DB8:2222:7223::72
Console(config)#
```

mvr6 vlan This command specifies the VLAN through which MVR multicast data is received. Use the **no** form of this command to restore the default MVR VLAN.

Syntax

mvr6 domain *domain-id* **vlan** *vlan-id*

no mvr6 domain *domain-id* **vlan**

domain-id - An independent multicast domain. (Range: 1-5)

vlan-id - Specifies the VLAN through which MVR multicast data is received. This is also the VLAN to which all source ports must be assigned. (Range: 1-4094)

Default Setting

VLAN 1

Command Mode

Global Configuration

Command Usage

MVR source ports can be configured as members of the MVR VLAN using the `switchport allowed vlan` command and `switchport native vlan` command, but MVR receiver ports should not be statically configured as members of this VLAN.

Example

The following example sets the MVR VLAN to VLAN 1:

```
Console(config)#mvr6 domain 1 vlan 1
Console(config)#
```

mvr6 immediate-leave This command causes the switch to immediately remove an interface from a multicast stream as soon as it receives a leave message for that group. Use the **no** form to restore the default settings.

Syntax

[no] mvr6 domain *domain-id* immediate-leave

domain-id - An independent multicast domain. (Range: 1-5)

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ Immediate leave applies only to receiver ports. When enabled, the receiver port is immediately removed from the multicast group identified in the leave message. When immediate leave is disabled, the switch follows the standard rules by sending a group-specific query to the receiver port and waiting for a response to determine if there are any remaining subscribers for that multicast group before removing the port from the group list.
- ◆ Using immediate leave can speed up leave latency, but should only be enabled on a port attached to only one multicast subscriber to avoid disrupting services to other group members attached to the same interface.
- ◆ Immediate leave does not apply to multicast groups which have been statically assigned to a port with the `mvr6 vlan group` command.

Example

The following enables immediate leave on a receiver port.

```
Console(config)#interface ethernet 1/5
Console(config-if)#mvr6 domain 1 immediate-leave
Console(config-if)#
```

mvr6 type This command configures an interface as an MVR receiver or source port. Use the **no** form to restore the default settings.

Syntax

[no] mvr6 domain *domain-id* type {receiver | source}

domain-id - An independent multicast domain. (Range: 1-5)

receiver - Configures the interface as a subscriber port that can receive multicast data.

source - Configures the interface as an uplink port that can send and receive multicast data for the configured multicast groups. Note that the source port must be manually configured as a member of the MVR6 VLAN using the [switchport allowed vlan](#) command.

Default Setting

The port type is not defined.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ A port configured as an MVR6 receiver or source port can join or leave multicast groups configured under MVR6. A port which is not configured as an MVR receiver or source port can use MLD snooping to join or leave multicast groups using the standard rules for multicast filtering (see [“MLD Snooping” on page 624](#)).
- ◆ Receiver ports can belong to different VLANs, but should not be configured as a member of the MVR VLAN. Also, note that VLAN membership for MVR receiver ports cannot be set to access mode (see the [switchport mode](#) command).
- ◆ One or more interfaces may be configured as MVR source ports. A source port is able to both receive and send data for multicast groups which it has joined through the MVR6 protocol or which have been assigned through the [mvr6 vlan group](#) command.

All source ports must belong to the MVR6 VLAN.

Subscribers should not be directly connected to source ports.

- ◆ The same port cannot be configured as a source port in one MVR domain and as a receiver port in another domain.

Example

The following configures one source port and several receiver ports on the switch.

```
Console(config)#interface ethernet 1/5
Console(config-if)#mvr6 domain 1 type source
Console(config-if)#exit
Console(config)#interface ethernet 1/6
Console(config-if)#mvr6 domain 1 type receiver
Console(config-if)#exit
Console(config)#interface ethernet 1/7
Console(config-if)#mvr6 domain 1 type receiver
Console(config-if)#
```

mvr6 vlan group This command statically binds a multicast group to a port which will receive long-term multicast streams associated with a stable set of hosts. Use the **no** form to restore the default settings.

Syntax

[no] mvr6 domain domain-id vlan vlan-id group ip-address

domain-id - An independent multicast domain. (Range: 1-5)

vlan-id - Receiver VLAN to which the specified multicast traffic is flooded. (Range: 1-4094)

group - Defines a multicast service sent to the selected port.

ip-address - Statically configures an interface to receive multicast traffic from the IPv6 address specified for an MVR multicast group. This parameter must be a full IPv6 address including the network prefix and host address bits.

Default Setting

No receiver port is a member of any configured multicast group.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ Multicast groups can be statically assigned to a receiver port using this command. The assigned address must fall within the range set by the **mvr6 associated-profile** command.
- ◆ All IPv6 addresses must be according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. (Note that the IP address ff02::X is reserved.)

- ◆ The MVR VLAN cannot be specified as the receiver VLAN for static bindings.

Example

The following statically assigns a multicast group to a receiver port:

```
Console(config)#interface ethernet 1/2
Console(config-if)#mvr6 domain 1 type receiver
Console(config-if)#mvr6 domain 1 vlan 2 group ff00::1
Console(config-if)#
```

clear mvr6 groups dynamic This command clears multicast group information dynamically learned through MVR.

Syntax

clear mvr groups dynamic

Command Mode

Privileged Exec

Command Usage

This command only clears entries learned through MVR. Statically configured multicast address are not cleared.

Example

```
Console#clear mvr6 groups r&d
Console#
```

clear mvr6 statistics This command clears MVR statistics.

Syntax

clear mvr statistics [**interface** *interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

vlan *vlan-id* - VLAN identifier (Range: 1-4094)

Command Mode

Privileged Exec

Example

```
Console#clear mvr6 statistics
Console#
```

show mvr6 This command shows information about MVR domain settings, including MVR operational status, the multicast VLAN, the current number of group addresses, and the upstream source IP address.

Syntax

show mvr6 [**domain** *domain-id*]

domain-id - An independent multicast domain. (Range: 1-5)

Default Setting

Displays configuration settings for all MVR domains.

Command Mode

Privileged Exec

Example

The following shows the MVR settings:

```
Console#show mvr6
MVR6 Proxy Switching      : Enabled
MVR6 Robustness Value     : 1
MVR6 Proxy Query Interval : 125(sec.)
MVR6 Source Port Mode     : Always Forward

MVR6 Domain              : 1
MVR6 Config Status       : Enabled
MVR6 Running Status      : Active
MVR6 Multicast VLAN      : 1
MVR6 Current Learned Groups : 0
MVR6 Upstream Source IP   : FF05::25
Console#
```

Table 137: show mvr6 - display description

Field	Description
MVR Proxy Switching	Shows if MVR proxy switching is enabled
MVR6 Proxy Query Interval	The interval at which the receiver port sends out general queries
MVR6 Source Port Mode	Shows if the switch only forwards multicast streams which the source port has dynamically joined or always forwards multicast streams
MVR Robustness Value	Shows the number of reports or query messages sent when proxy switching is enabled
MVR6 Domain	An independent multicast domain.

Table 137: show mvr6 - display description (Continued)

Field	Description
MVR6 Config Status	Shows if MVR is globally enabled on the switch.
MVR6 Running Status	Indicates whether or not all necessary conditions in the MVR environment are satisfied. (Running status is true as long as MVR Status is enabled, and the specified MVR VLAN exists, and a source port with a valid link has been configured (using the <code>mvr6 type</code> command.)
MVR6 Multicast VLAN	Shows the VLAN used to transport all MVR multicast traffic.
MVR Current Learned Groups	The current number of MVR group addresses
MVR6 Upstream Source IP	The source IP address assigned to all upstream control packets.

show mvr6 associated-profile This command shows the profiles bound the specified domain.

Syntax

show mvr6 [domain domain-id] associated-profile

domain-id - An independent multicast domain. (Range: 1-5)

Default Setting

Displays profiles bound to all MVR domains.

Command Mode

Privileged Exec

Example

The following displays the profiles bound to domain 1:

```
Console#show mvr6 domain 1 associated-profile
Domain ID : 1
MVR Profile Name      Start IPv6 Addr.      End IPv6 Addr.
-----
rd                     FF00::1                FF00::9
Console#
```

show mvr6 interface This command shows MVR configuration settings for interfaces attached to the MVR VLAN.

Syntax

show mvr6 [domain domain-id] interface

domain-id - An independent multicast domain. (Range: 1-5)

Default Setting

Displays configuration settings for all attached interfaces.

Command Mode

Privileged Exec

Example

The following displays information about the interfaces attached to the MVR VLAN in domain 1:

```

Console#show mvr6 domain 1 interface
MVR6 Domain : 1
Port      Type      Status      Immediate  Static Group Address
-----
Eth1/ 1   Source   Active/Up
Eth1/ 2   Receiver Active/Up   Disabled   FF00::1 (VLAN2)
Console#

```

Table 138: show mvr6 interface - display description

Field	Description
Port	Shows interfaces attached to the MVR.
Type	Shows the MVR port type.
Status	Shows the MVR status and interface status. MVR status for source ports is "ACTIVE" if MVR is globally enabled on the switch. MVR status for receiver ports is "ACTIVE" only if there are subscribers receiving multicast traffic from one of the MVR groups, or a multicast group has been statically assigned to an interface.
Immediate	Shows if immediate leave is enabled or disabled.
Static Group Address	Shows any static MVR group assigned to an interface, and the receiver VLAN.

show mvr6 members This command shows information about the current number of entries in the forwarding database, or detailed information about a specific multicast address.

Syntax

show mvr6 [**domain** *domain-id*] **members** [*ip-address*]

domain-id - An independent multicast domain. (Range: 1-5)

ip-address - IPv6 address for an MVR multicast group.

Default Setting

Displays configuration settings for all domains and all forwarding entries.

Command Mode

Privileged Exec

Example

The following shows information about the number of multicast forwarding entries currently active in domain 1:

```

Console#show mvr6 domain 1 members
MVR6 Domain : 1
MVR6 Forwarding Entry Count :1
Flag: S - Source port, R - Receiver port.
      H - Host counts (number of hosts join the group on this port).
      P - Port counts (number of ports join the group).
Up time: Group elapsed time (d:h:m:s).
Expire : Group remaining time (m:s).

Group Address          VLAN Port          Up time          Expire Count
-----
FF00::1                1
                        1 Eth1/ 1(S)
                        2 Eth1/ 2(S)
Console#

```

The following example shows detailed information about a specific multicast address:

```

Console#show mvr6 domain 1 members ff00::1
MVR6 Domain : 1
MVR6 Forwarding Entry Count :1
Flag: S - Source port, R - Receiver port.
      H - Host counts (number of hosts join the group on this port).
      P - Port counts (number of ports join the group).
Up time: Group elapsed time (d:h:m:s).
Expire : Group remaining time (m:s).

Group Address          VLAN Port          Up time          Expire Count
-----
FF00::1                1
                        1 Eth1/ 1(S)
                        2 Eth1/ 2(S)
Console#

```

Table 139: show mvr6 members - display description

Field	Description
Group Address	Multicast group address.
VLAN	VLAN to which this address is forwarded.
Port	Port to which this address is forwarded.
Up time	Time that this multicast group has been known.
Expire	The time until this entry expires.
Count	The number of times this address has been learned by MVR (MLD snooping).

show mvr6 profile This command shows all configured MVR profiles.

Command Mode

Privileged Exec

Example

The following shows all configured MVR profiles:

```

Console#show mvr6 profile
MVR Profile Name      Start IPv6 Addr.      End IPv6 Addr.
-----
rd                      FF00::1                FF00::9
Console#

```

show mvr6 statistics This command shows MVR protocol-related statistics for the specified interface.

Syntax

show mvr6 statistics {input | output} [interface *interface*]

show mvr6 domain *domain-id* **statistics**

{input [interface *interface*] | output [interface *interface*] |
query}

domain-id - An independent multicast domain. (Range: 1-5)

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

vlan *vlan-id* - VLAN ID (Range: 1-4094)

query - Displays MVR query-related statistics.

Default Setting

Displays statistics for all domains.

Command Mode

Privileged Exec

Example

The following shows MVR protocol-related statistics received:

```

Console#show mvr6 domain 1 statistics input
MVR Domain : 1
Input Statistics:
Interface Report    Leave    G Query  G(-S)-S Query Drop    Join Succ Group
-----
Eth 1/ 1           23       11        4         10        5        20        9
Eth 1/ 2           12       15        8          3        5        19        4
VLAN 1             2        0         0          2        2        20        9
Console#

```

Table 140: show mvr6 statistics input - display description

Field	Description
Interface	Shows interfaces attached to the MVR.
Report	The number of IGMP membership reports received on this interface.
Leave	The number of leave messages received on this interface.
G Query	The number of general query messages received on this interface.
G(-S)-S Query	The number of group specific or group-and-source specific query messages received on this interface.
Drop	The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR group report received
Join Succ	The number of times a multicast group was successfully joined.
Group	The number of MVR groups active on this interface.

The following shows MVR protocol-related statistics sent:

```

Console#show mvr6 domain 1 statistics output
MVR Domain : 1
Output Statistics:
Interface Report    Leave    G Query  G(-S)-S Query
-----
Eth 1/ 1           12        0         1          0
Eth 1/ 2           5         1         4          1
VLAN 1             7         2         3          0
Console#

```

Table 141: show mvr6 statistics output - display description

Field	Description
Interface	Shows interfaces attached to the MVR.
Report	The number of IGMP membership reports sent from this interface.
Leave	The number of leave messages sent from this interface.

Table 141: show mvr6 statistics output - display description (Continued)

Field	Description
G Query	The number of general query messages sent from this interface.
G(-S)-S Query	The number of group specific or group-and-source specific query messages sent from this interface.

The following shows MVR query-related statistics:

```

Console#show mvr6 domain 1 statistics query
Querier IPv6 Address      : FE80::2E0:CFF:FE00:FB/64
Querier Expire Time       : 00(h):00(m):30(s)
General Query Received    : 10
General Query Sent        : 0
Specific Query Received   : 2
Specific Query Sent       : 0
Number of Reports Sent    : 2
Number of Leaves Sent     : 0
Console#

```

IGMP (Layer 3)

This section describes commands used to configure Layer 3 Internet Group Management Protocol (IGMP) on the switch.

Table 142: IGMP Commands (Layer 3)

Command	Function	Mode
<code>ip igmp</code>	Enables IGMP for the specified interface	IC
<code>ip igmp last-member-query-interval</code>	Configures the frequency at which to send query messages in response to receiving a leave message	IC
<code>ip igmp max-resp-interval</code>	Configures the maximum host response time	IC
<code>ip igmp query-interval</code>	Configures frequency for sending host query messages	IC
<code>ip igmp robustval</code>	Configures the expected packet loss	IC
<code>ip igmp static-group</code>	Configures the router to be a static member of a multicast group on the specified VLAN interface	IC
<code>ip igmp version</code>	Configures IGMP version used on this interface	IC
<code>clear ip igmp group</code>	Deletes entries from the IGMP cache	PE
<code>show ip igmp groups</code>	Displays information for IGMP groups	PE
<code>show ip igmp interface</code>	Displays multicast information for the specified interface	PE

ip igmp This command enables IGMP on a VLAN interface. Use the **no** form of this command to disable IGMP on the specified interface.

Syntax

[no] ip igmp

Default Setting

Disabled

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ IGMP (including query functions) can be enabled for specific VLAN interfaces at Layer 3 through the **ip igmp** command.
- ◆ When a multicast routing protocol, such as PIM - Dense Mode, is enabled, IGMP is also enabled.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip igmp
Console(config-if)#end
Console#show ip igmp interface
  IGMP                               : Enabled
  IGMP Version                       : 2
  IGMP Proxy                         : Disabled
  IGMP Unsolicited Report Interval   : 400 sec
  Robustness Variable                 : 2
  Query Interval                     : 125 sec
  Query Max Response Time             : 100 (resolution in 0.1 sec)
  Last Member Query Interval         : 10 (resolution in 0.1 sec)
  Querier                            : 0.0.0.0
  Joined Groups :
  Static Groups :
```

Console#

Related Commands

[ip igmp snooping \(593\)](#)

[show ip igmp snooping \(608\)](#)

ip igmp last-member-query-interval This command configures the frequency at which to send IGMP group-specific or IGMPv3 group-source-specific query messages in response to receiving a group-specific or group-source-specific leave message. Use the **no** form to restore the default setting.

Syntax

ip igmp last-member-query-interval *seconds*

no ip igmp last-member-query-interval

seconds - The frequency at which the switch sends group-specific or group-source-specific queries upon receipt of a leave message. (Range: 1-255 tenths of a second)

Default Setting

10 (1 second)

Command Mode

Interface Configuration (VLAN)

Command Usage

When the switch receives an IGMPv2 or IGMPv3 leave message from a host that wants to leave a multicast group, source or channel, it sends a number of group-specific or group-source-specific query messages at intervals defined by this command. If no response is received after this period, the switch stops forwarding for the group, source or channel.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip igmp last-member-query-interval 20
Console(config-if)#
```

ip igmp max-resp-interval This command configures the maximum response time advertised in IGMP queries. Use the **no** form of this command to restore the default.

Syntax

ip igmp max-resp-interval *seconds*

no ip igmp max-resp-interval

seconds - The report delay advertised in IGMP queries. (Range: 0-255 tenths of a second)

Default Setting

100 (10 seconds)

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ IGMPv1 does not support a configurable maximum response time for query messages. It is fixed at 10 seconds for IGMPv1.
- ◆ By varying the Maximum Response Interval, the burstiness of IGMP messages passed on the subnet can be tuned; where larger values make the traffic less bursty, as host responses are spread out over a larger interval.
- ◆ The number of seconds represented by the maximum response interval must be less than the Query Interval ([page 674](#)).

Example

The following shows how to configure the maximum response time to 20 seconds.

```
Console(config-if)#ip igmp query-max-response-time 200
Console(config-if)#
```

Related Commands

[ip igmp version \(677\)](#)

[ip igmp query-interval \(674\)](#)

ip igmp query-interval This command configures the frequency at which host query messages are sent. Use the **no** form to restore the default.

Syntax

ip igmp query-interval *seconds*

no ip igmp query-interval

seconds - The frequency at which the switch sends IGMP host-query messages. (Range: 1-255 seconds)

Default Setting

125 seconds

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ Multicast routers send host query messages to determine the interfaces that are connected to downstream hosts requesting a specific multicast service. Only the designated multicast router for a subnet sends host query messages, which are addressed to the multicast address 224.0.0.1, and uses a time-to-live (TTL) value of 1.
- ◆ For IGMP Version 1, the designated router is elected according to the multicast routing protocol that runs on the LAN. But for IGMP Version 2 and 3, the designated querier is the lowest IP-addressed multicast router on the subnet.

Example

The following shows how to configure the query interval to 100 seconds.

```
Console(config-if)#ip igmp query-interval 100
Console(config-if)#
```

Related Commands

[ip igmp max-resp-interval \(673\)](#)

ip igmp robustval This command specifies the robustness (expected packet loss) for this interface. Use the **no** form of this command to restore the default value.

Syntax

ip igmp robustval *robust-value*

no ip igmp robustval

robust-value - The robustness of this interface. (Range: 1-255)

Default Setting

2

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ The robustness value is used in calculating the appropriate range for other IGMP variables, such as the Group Membership Interval, as well as the Other Querier Present Interval, and the Startup Query Count (RFC 3376).
- ◆ Routers adopt the robustness value from the most recently received query. If the querier's robustness variable (QRV) is zero, indicating that the QRV field does not contain a declared robustness value, the switch will set the robustness variable to the value statically configured by this command. If the QRV exceeds 7, the maximum value of the QRV field, the robustness value is set to zero, meaning that this device will not advertise a QRV in any query messages it subsequently sends.

Example

```
Console(config-if)#ip igmp robustness-variable 3
Console(config-if)#
```

ip igmp static-group This command configures the router to be a static member of a multicast group on the specified VLAN interface. Use the **no** form to remove the static mapping.

Syntax

ip igmp static-group *group-address* [**source** *source-address*]

no ip igmp static-group

group-address - IP multicast group address. (The group addresses specified cannot be in the range of 224.0.0.1 - 239.255.255.255.)

source-address - Source address for a multicast server transmitting traffic to the corresponding multicast group address.

Default Setting

None

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ Group addresses within the entire multicast group address range can be specified with this command. However, if any address within the source-specific multicast (SSM) address range (default 232/8) is specified, but no source address is included in the command, the request to join the multicast group will fail unless the next node up the reverse path tree has statically mapped this group to a specific source address. Also, if an address outside of the SSM address range is specified, and a specific source address is included in the command, the request to join the multicast group will also fail if the next node up the reverse path tree has enabled the PIM-SSM protocol.
- ◆ If a static group is configured for an any-source multicast (*,G), a source address cannot subsequently be defined for this group without first deleting the entry.
- ◆ If a static group is configured for one or more source-specific multicasts (S,G), an any-source multicast (*,G) cannot subsequently be defined for this group without first deleting all of the associated (S,G) entries.
- ◆ Using the **no** form of this command to delete a static group without specifying the source address will delete all any-source and source-specific multicast entries for the specified group.
- ◆ The switch supports a maximum of 16 static group entries.

Example

The following example assigns VLAN 1 as a static member of the specified multicast group.

```
Console(config)#interface vlan1
Console(config-if)#ip igmp static-group 225.1.1.1
```

ip igmp version This command configures the IGMP version used on an interface. Use the **no** form of this command to restore the default.

Syntax

ip igmp version {1 | 2 | 3}

no ip igmp version

1 - IGMP Version 1

2 - IGMP Version 2

3 - IGMP Version 3

Default Setting

IGMP Version 2

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ All routers on the subnet must support the same version. However, the multicast hosts on the subnet may support any of the IGMP versions 1 - 3.
- ◆ If the switch receives an IGMP Version 1 Membership Report, it sets a timer to note that there are Version 1 hosts which are members of the group for which it heard the report.

If there are Version 1 hosts present for a particular group, the switch will ignore any Leave Group messages that it receives for that group.

Example

```
Console(config-if)#ip igmp version 1
Console(config-if)#
```

clear ip igmp group This command deletes entries from the IGMP cache.

Syntax

clear ip igmp group [*group-address* | **interface** *interface*]

group-address - IP address of the multicast group.

interface

vlan *vlan-id* - VLAN ID. (Range: 1-4094)

Default Setting

Deletes all entries in the cache if no options are selected.

Command Mode

Privileged Exec

Command Usage

Enter the address for a multicast group to delete all entries for the specified group.
Enter the interface option to delete all multicast groups for the specified interface.
Enter no options to clear all multicast groups from the cache.

Example

The following example clears all multicast group entries for VLAN 1.

```
Console#clear ip igmp interface vlan1
Console#
```

show ip igmp groups This command displays information on multicast groups active on the switch and learned through IGMP.

Syntax

show ip igmp groups [{*group-address* | *interface*} [**detail**] | **detail**]

group-address - IP multicast group address.

interface

vlan *vlan-id* - VLAN ID. (Range: 1-4094)

detail - Displays detailed information about the multicast process and source addresses when available.

Command Mode

Privileged Exec

Command Usage

To display information about multicast groups, IGMP must first be enabled on the interface to which a group has been assigned using the [ip igmp](#) command, and multicast routing must be enabled globally on the system using the [ip multicast-routing](#) command.

Example

The following shows options for displaying IGMP group information by interface, group address, and static listing.

```
Console#show ip igmp groups
Group Address  Interface VLAN  Last Reporter  Uptime  Expire  V1 Timer
-----
    224.0.17.17             1    192.168.1.10   0:0:1   0:4:19   0:0:0
Console#show ip igmp groups 234.5.6.8
Group Address  Interface VLAN  Last Reporter  Uptime  Expire  V1 Timer
-----
    224.0.17.17             1    192.168.1.10   0:0:1   0:4:19   0:0:0
```

```

Console#show ip igmp groups interface vlan 1
Group Address      Interface VLAN  Last Reporter    Uptime    Expire    V1 Timer
-----
      224.0.17.17          1    192.168.1.10    0:0:1     0:4:19    0:0:0
Console#

```

Table 143: show ip igmp groups - display description

Field	Description
Group Address	IP multicast group address with subscribers directly attached or downstream from the switch.
Interface VLAN	The interface on the switch that has received traffic directed to the multicast group address.
Last Reporter	The IP address of the source of the last membership report received for this multicast group address on this interface.
Uptime	The time elapsed since this entry was created.
Expire	The time remaining before this entry will be aged out. (The default is 260 seconds.) This field displays “stopped” if the Group Mode is INCLUDE.
V1 Timer	The time remaining until the switch assumes that there are no longer any IGMP Version 1 members on the IP subnet attached to this interface. <ul style="list-style-type: none"> ♦ If the switch receives an IGMP Version 1 Membership Report, it sets a timer to note that there are Version 1 hosts present which are members of the group for which it heard the report. ♦ If there are Version 1 hosts present for a particular group, the switch will ignore any Leave Group messages that it receives for that group.

The following shows the information displayed in a detailed listing for a dynamically learned multicast group.

```

Console#show ip igmp groups detail
Interface      : VLAN 1
Group          : 224.1.2.3
Uptime         : 0h:0m:12s
Group mode     : Include
Last reporter  : 0.0.0.0
Group Source List:
Source Address  Uptime      v3  Exp      Fwd
-----
      192.1.2.3    0h:0m:12s    0h:0m:0s  Yes
Console#

```

Table 144: show ip igmp groups detail - display description

Field	Description
Interface	The interface on the switch that has received traffic directed to the multicast group address.
Group	IP multicast group address with subscribers directly attached or downstream from the switch, or a static multicast group assigned to this interface.

Table 144: show ip igmp groups detail - display description (Continued)

Field	Description
Uptime	The time elapsed since this entry was created.
Group mode	In INCLUDE mode, reception of packets sent to the specified multicast address is requested only from those IP source addresses listed in the source-list parameter. In EXCLUDE mode, reception of packets sent to the given multicast address is requested from all IP source addresses except for those listed in the source-list parameter, and where the source timer status has expired. Note that EXCLUDE mode does not apply to SSM addresses.
Last Reporter	The IP address of the source of the last membership report received for this multicast group address on this interface.
Group Source List	A list of zero or more IP unicast addresses from which multicast reception is desired or not desired, depending on the filter mode.
Source Address	The address of one of the multicast servers transmitting traffic to the specified group.
Uptime	The time elapsed since this entry was created.
v3 Exp	The time remaining before this entry will be aged out. The V3 label indicates that the expire time is only provided for sources learned through IGMP Version 3. (The default is 260 seconds.)
Fwd	Indicates whether or not traffic will be forwarded from the multicast source.

show ip igmp interface This command shows multicast information for the specified interface.

Syntax

show ip igmp interface [*interface*]
interface
vlan *vlan-id* - VLAN ID. (Range: 1-4094)

Default Setting

None

Command Mode

Privileged Exec

Example

The following example shows the IGMP configuration for VLAN 1, as well as the device currently serving as the IGMP querier for active multicast services on this interface.

```
switch#show ip igmp interface vlan 1
Vlan 1 : up
  IGMP                               : Disabled
  IGMP Version                       : 2
  IGMP Proxy                         : Enabled
  IGMP Unsolicited-report-interval   : 400 sec
  Robustness variable                 : 2
```



```
Query Interval                : 125 sec
Query Max Response Time       : 100 (resolution in 0.1 sec)
Last Member Query Interval    : 10 (resolution in 0.1 sec)
Querier                       : 0.0.0.0
Joined Groups :
Static Groups :
switch#
```

IGMP Proxy Routing

This section describes commands used to configure IGMP Proxy Routing on the switch.

Table 145: IGMP Proxy Commands

Command	Function	Mode
<code>ip igmp proxy</code>	Enables IGMP proxy service for multicast routing	IC
<code>ip igmp proxy unsolicited-report-interval</code>	Specifies how often the upstream interface should transmit unsolicited IGMP reports	IC
<code>show ip igmp interface</code>	Displays multicast information for the specified interface	PE

To enable IGMP proxy service, follow these steps:

1. Use the `ip multicast-routing` command to enable IP multicasting globally on the router.
2. Use the `ip igmp proxy` command to enable IGMP proxy on the upstream interface that is attached to an upstream multicast router.
3. Use the `ip igmp` command to enable IGMP on the downstream interfaces from which to forward IGMP membership reports.
4. Optional – Use the `ip igmp proxy unsolicited-report-interval` command to indicate how often the system will send unsolicited reports to the upstream router.

ip igmp proxy This command enables IGMP proxy service for multicast routing, forwarding IGMP membership information monitored on downstream interfaces onto the upstream interface in a summarized report. Use the **no** form to disable proxy service.

Syntax

[no] ip igmp proxy

Default Setting

Disabled

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ When IGMP proxy is enabled on an interface, that interface is known as the upstream or host interface. This interface performs only the host portion of IGMP by sending IGMP membership reports, and automatically disables IGMP router functions.
- ◆ Interfaces with IGMP enabled, but not located in the direction of the multicast tree root are known as downstream or router interfaces. These interfaces perform the standard IGMP router functions by maintaining a database of all IGMP subscriptions on the downstream interface. IGMP must therefore be enabled on all downstream interfaces which require proxy multicast service.
- ◆ When changes occur in the downstream IGMP groups, a IGMP state change report is created and sent to the upstream router.
- ◆ If there is an IGMPv1 or IGMPv2 querier on the upstream network, then the proxy device will act as an IGMPv1 or IGMPv2 host on the upstream interface accordingly. Otherwise, it will act as an IGMPv3 host.
- ◆ Multicast routing protocols are not supported on interfaces where IGMP proxy service is enabled.
- ◆ Only one upstream interface is supported on the system.
- ◆ A maximum of 1024 multicast streams are supported.

Example

The following example enables multicast routing globally on the switch, configures VLAN 2 as a downstream interface, and then VLAN 1 as the upstream interface.

```
Console(config)#ip multicast-routing
Console(config)#interface vlan2
Console(config-if)#ip igmp
Console(config-if)#exit
Console(config)#interface vlan1
Console(config-if)#ip igmp proxy
Console(config-if)#
```

ip igmp proxy unsolicited-report-interval This command specifies how often the upstream interface should transmit unsolicited IGMP reports. Use the **no** form to restore the default value.

Syntax

ip igmp proxy unsolicited-report-interval *seconds*

no ip igmp proxy unsolicited-report-interval

seconds - The interval at which to issue unsolicited reports.
(Range: 1-65535 seconds)

Default Setting

400 seconds

Command Mode

Interface Configuration (VLAN)

Example

The following example sets the interval for sending unsolicited IGMP reports to 5 seconds.

```
switch(config)#interface vlan
switch(config-if)#ip igmp proxy unsolicited-report-interval 5
switch(config)#
```

MLD (Layer 3)

This section describes commands used to configure Layer 3 Multicast Listener Discovery (MLD) on the switch.

Table 146: MLD Commands (Layer 3)

Command	Function	Mode
ipv6 mld	Enables MLD for the specified interface	IC
ipv6 mld last-member-query-response-interval	Configures the frequency at which to send query messages in response to receiving a leave message	IC
ipv6 mld max-resp-interval	Configures the maximum host response time	IC
ipv6 mld query-interval	Configures frequency for sending host query messages	IC
ipv6 mld robustval	Configures the expected packet loss	IC
ipv6 mld static-group	Statically binds multicast groups to a VLAN interface	IC
ipv6 mld version	Configures MLD version used on an interface	IC
clear ipv6 mld group	Deletes entries from the MLD cache	PE
show ipv6 mld groups	Displays information for MLD groups	PE
show ip igmp interface	Displays multicast information for an interface	PE

ipv6 mld This command enables MLD on a VLAN interface. Use the **no** form of this command to disable MLD on the selected interface.

Syntax

[no] ipv6 mld

Default Setting

Disabled

Command Mode

Interface Configuration (VLAN)

Command Usage

MLD (including query functions) can be enabled for specific VLAN interfaces at Layer 3 through the **ipv6 mld** command.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 mld
Console(config-if)#end
Console#show ipv6 mld interface
VLAN 1 : Up
    MLD                               : Enabled
    MLD Version                       : 2
    MLD Proxy                         : Disabled
    MLD Unsolicited Report Interval   : 400 sec
    Robustness Variable               : 2
    Query Interval                    : 125 sec
    Query Max Response Time           : 10 sec
    Last Member Query Interval        : 1 sec
    Querier                           : ::
    Joined Groups :
    Static Groups :
```

Console#

ipv6 mld last-member-query-response-interval This command configures the frequency at which to send MLD group-specific or MLDv2 group-source-specific query messages in response to receiving a group-specific or group-source-specific leave message from the last known active host on the subnet. Use the **no** form to restore the default setting.

Syntax

ipv6 mld last-member-query-response-interval *seconds*

no ipv6 mld last-member-query-response-interval

seconds - The frequency at which the switch sends group-specific or group-source-specific queries upon receipt of a leave message. (Range: 1-255 seconds)

Default Setting

10 (1 second)

Command Mode

Interface Configuration (VLAN)

Command Usage

When the switch receives an MLD or MLDv2 leave message from a host that wants to leave a multicast group, source or channel, it sends a number of group-specific or group-source-specific query messages at intervals defined by this command. If no response is received after this period, the switch stops forwarding for the group, source or channel.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 mld last-member-query-response-interval 20
Console(config-if)#
```

ipv6 mld max-resp-interval This command configures the maximum response time advertised in MLD queries. Use the **no** form of this command to restore the default setting.

Syntax**ipv6 mld max-resp-interval** *seconds***no ipv6 mld max-resp-interval**

seconds - The report delay advertised in MLD queries.
(Range: 0-255 tenths of a second)

Default Setting

100 (10 seconds)

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ By varying the Maximum Response Interval, the burstiness of MLD messages passed on the subnet can be tuned; where larger values make the traffic less bursty, as host responses are spread out over a larger interval.
- ◆ The number of seconds represented by the maximum response interval must be less than the Query Interval ([page 686](#)).

Example

The following shows how to configure the maximum response time to 20 seconds.

```
Console(config-if)#ipv6 mld max-resp-interval 200  
Console(config-if)#
```

Related Commands

[ipv6 mld query-interval \(686\)](#)

ipv6 mld query-interval This command configures the frequency at which host query messages are sent. Use the **no** form to restore the default.

Syntax

ipv6 mld query-interval *seconds*

no ipv6 mld query-interval

seconds - The frequency at which the switch sends MLD host-query messages. (Range: 1-255 seconds)

Default Setting

125 seconds

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ Multicast routers send host query messages to determine the interfaces that are connected to downstream hosts requesting a specific multicast service. Only the designated multicast router for a subnet sends host query messages, which are addressed to the link-scope all-nodes multicast address FF02::1, and uses a time-to-live (TTL) value of 1.
- ◆ The designated querier is the lowest IP-addressed multicast router on the subnet.

Example

The following shows how to configure the query interval to 100 seconds.

```
Console(config-if)#ipv6 mld query-interval 100  
Console(config-if)#
```

Related Commands

[ipv6 mld max-resp-interval \(685\)](#)

ipv6 mld robustval This command specifies the robustness (expected packet loss) for this interface. Use the **no** form of this command to restore the default value.

Syntax

ipv6 mld robustval *robust-value*

no ipv6 mld robustval

robust-value - The robustness of this interface. (Range: 1-255)

Default Setting

2

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ The robustness value is used to compensate for expected packet loss on a link. It indicates the number of refresh packets related to the current MLD state which might be lost without having to terminate that state.
- ◆ Routers adopt the robustness value from the most recently received query. If the query's robustness variable (QRV) is zero, indicating that the QRV field does not contain a declared robustness value, the switch will set the robustness variable to the value statically configured by this command. If the QRV exceeds 7, the maximum value of the QRV field, the robustness value is set to zero, meaning that this device will not advertise a QRV in any query messages it subsequently sends.

Example

```
Console(config-if)#ipv6 mld robustval 3
Console(config-if)#
```

ipv6 mld static-group This command statically binds multicast groups to a VLAN interface. Use the **no** form to remove the static mapping.

Syntax

ipv6 mld static-group *group-address* [**source** *source-address*]

no ipv6 mld static-group [*group-address* [**source** *source-address*]]

group-address - IPv6 multicast group address. (Note that link-local scope addresses FF02:* are not allowed.)

source-address - IPv6 source address for a multicast server transmitting traffic to the corresponding multicast group address.

Default Setting

None

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ If a static group is configured for an any-source multicast (*,G), a source address cannot subsequently be defined for this group without first deleting the entry.
- ◆ If a static group is configured for one or more source-specific multicasts (S,G), an any-source multicast (*,G) cannot subsequently be defined for this group without first deleting all of the associated (S,G) entries.
- ◆ Use the **no** form of this command without specifying a group address to delete all any-source and source-specific multicast entries.
- ◆ Use the **no** form of this command to delete a static group without specifying the source address to delete all any-source and source-specific multicast entries for the specified group.
- ◆ The switch supports a maximum of 64 static group entries.

Example

The following example assigns VLAN 1 as a static member of the specified multicast group.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 mld static-group FFEE::0101
Console(config-if)#
```

ipv6 mld version This command configures the MLD version used on an interface. Use the **no** form of this command to restore the default setting.

Syntax

ipv6 mld version {1 | 2}

no ipv6 mld version

1 - MLD Version 1

2 - MLD Version 2

Default Setting

MLD Version 2

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ MLDv1 is derived from IGMPv2, and MLDv2 from IGMPv3. IGMP uses IP Protocol 2 message types, and MLD uses IP Protocol 58 message types, which is a subset of the ICMPv6 messages.
- ◆ MLDv2 adds the ability for a node to report interest in listening to packets with a particular multicast address only from specific source addresses as required to support Source-Specific Multicast (SSM), or from all sources except for specific source addresses.
- ◆ MLDv2 supports Source-Specific Multicast (SSM) which builds a reverse tree from a host requesting a service back up to the multicast server.
- ◆ Multicast hosts on the subnet may support either MLD versions 1 or 2.

Example

```
Console(config-if)#ipv6 mld version 1
Console(config-if)#
```

clear ipv6 mld group This command deletes entries from the MLD cache.

Syntax

clear ipv6 mld group [*group-address* | **interface** *interface*]

group-address - IPv6 address of the multicast group.

interface

vlan *vlan-id* - VLAN ID. (Range: 1-4094)

Default Setting

Deletes all entries in the cache if no options are selected.

Command Mode

Privileged Exec

Command Usage

Enter the address for a multicast group to delete all entries for the specified group. Enter the interface option to delete all multicast groups for the specified interface. Enter no options to clear all multicast groups from the cache.

Example

The following example clears all multicast group entries for VLAN 1.

```
Console#clear ipv6 mld interface vlan 1
Console#
```

show ipv6 mld groups This command displays information on multicast groups active on the switch and learned through MLD.

Syntax

show ipv6 mld groups [{*group-address* | *interface*] [**detail**] | **detail**]

group-address - IPv6 multicast group address. (Note that link-local scope addresses FF02:* are not allowed.)

interface

vlan *vlan-id* - VLAN ID. (Range: 1-4094)

detail - Displays detailed information about the multicast process and source addresses when available.

Command Mode

Privileged Exec

Command Usage

To display information about multicast groups, MLD must first be enabled on the interface to which a group has been assigned using the [ipv6 mld](#) command, and multicast routing must be enabled globally on the system using the [ip multicast-routing](#) command.

Example

The following shows options for displaying MLD group information.

```
Console#show ipv6 mld groups

Group Address                Interface VLAN  Uptime    Expire
-----
                                FFEE::101                1    0:1:59    Never

Console#show ipv6 mld groups detail
Interface      : VLAN 1
Group          : FFEE::101
Uptime        : 0h:2m:7s
Group Mode     : Include
Last Reporter  : FE80::0101
Group Source List:
Source Address                Uptime    Expire    Fwd
-----
                                FFEE::0101 0h:0m:12s 0h:0m:0s Yes

Console#
```

Table 147: show ipv6 mld groups - display description

Field	Description
Group Address	IP multicast group address with subscribers directly attached or downstream from the switch.
Interface VLAN	The interface on the switch that has received traffic directed to the multicast group address.
Uptime	The time elapsed since this entry was created.

Table 147: show ipv6 mld groups - display description (Continued)

Field	Description
Expire	The time remaining before this entry will be aged out. (The default is 260 seconds.) This field displays “stopped” if the Group Mode is INCLUDE.
Group Mode	In Include mode, reception of packets sent to the specified multicast address is requested only from those IP source addresses listed in the source-list parameter. In Exclude mode, reception of packets sent to the given multicast address is requested from all IP source addresses except for those listed in the source-list parameter, and where the source timer status has expired. Note that Exclude mode does not apply to SSM addresses.
Last Reporter	The IP address of the source of the last membership report received for this multicast group address on this interface.
Group Source List	A list of zero or more IP unicast addresses from which multicast reception is desired or not desired, depending on the filter mode.
Source Address	The address of one of the multicast servers transmitting traffic to the specified group.
Fwd	Indicates whether or not traffic will be forwarded from the multicast source.

show ipv6 mld interface This command shows multicast information for the specified interface.

Syntax

show ipv6 mld interface [*interface*]

interface

vlan *vlan-id* - VLAN ID. (Range: 1-4094)

Default Setting

None

Command Mode

Privileged Exec

Example

The following example shows the MLD configuration for VLAN 1, as well as the device currently serving as the MLD querier for active multicast services on this interface.

```

Console#show ipv6 mld interface vlan 1
VLAN 1 : Up
  MLD                               : Enabled
  MLD Version                       : 2
  MLD Proxy                         : Disabled
  MLD Unsolicited Report Interval   : 400 sec
  Robustness Variable               : 2
  Query Interval                    : 125 sec
  Query Max Response Time           : 10
  Last Member Query Interval        : 1

```

```
Querier                               : FE80::200:E8FF:FE93:82A0
Joined Groups :
Static Groups :
  FFEE::101
Console#
```

MLD Proxy Routing

This section describes commands used to configure MLD Proxy Routing on the switch.

Table 148: IGMP Proxy Commands

Command	Function	Mode
<code>ipv6 mld proxy</code>	Enables MLD proxy service for multicast routing	IC
<code>ipv6 mld proxy unsolicited-report-interval</code>	Specifies how often the upstream interface should transmit unsolicited IGMP reports	IC
<code>show ipv6 mld interface</code>	Displays multicast information for the specified interface	PE

To enable MLD proxy service, follow these steps:

1. Use the `ipv6 multicast-routing` command to enable IP multicasting globally on the router.
2. Use the `ipv6 mld proxy` command to enable MLD proxy on the upstream interface that is attached to an upstream multicast router.
3. Use the `ipv6 mld` command to enable MLD on the downstream interfaces from which to forward MLD membership reports.
4. Optional – Use the `ipv6 mld proxy unsolicited-report-interval` command to indicate how often the system will send unsolicited reports to the upstream router.

ipv6 mld proxy This command enables MLD proxy service for multicast routing, forwarding MLD membership information monitored on downstream interfaces onto the upstream interface in a summarized report. Use the **no** form to disable proxy service.

Syntax

[no] ipv6 mld proxy

Default Setting

Disabled

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ When MLD proxy is enabled on an interface, that interface is known as the upstream or host interface. This interface performs only the host portion of MLD by sending MLD membership reports, and automatically disables MLD router functions.
- ◆ Interfaces with MLD enabled, but not located in the direction of the multicast tree root are known as downstream or router interfaces. These interfaces perform the standard MLD router functions by maintaining a database of all MLD subscriptions on the downstream interface. MLD must therefore be enabled on all downstream interfaces which require proxy multicast service.
- ◆ When changes occur in the downstream MLD groups, an MLD state change report is created and sent to the upstream router.
- ◆ If there is an MLDv1 querier on the upstream network, then the proxy device will act as an MLDv1 host on the upstream interface accordingly. Otherwise, it will act as an MLDv2 host.
- ◆ Multicast routing protocols are not supported on interfaces where MLD proxy service is enabled.
- ◆ Only one upstream interface is supported on the system.
- ◆ MLD and MLD proxy cannot be enabled on the same interface.
- ◆ A maximum of 1024 multicast streams are supported.

Example

The following example enables multicast routing globally on the switch, configures VLAN 2 as a downstream interface, and then VLAN 1 as the upstream interface.

```
Console(config)#ip multicast-routing
Console(config)#interface vlan2
Console(config-if)#ipv6 mld
Console(config-if)#exit
Console(config)#interface vlan1
Console(config-if)#ipv6 mld proxy
Console(config-if)#
```

ipv6 mld proxy unsolicited-report-interval This command specifies how often the upstream interface should transmit unsolicited MLD reports. Use the **no** form to restore the default value.

Syntax

ipv6 mld proxy unsolicited-report-interval *seconds*

no ipv6 mld proxy unsolicited-report-interval

seconds - The interval at which to issue unsolicited reports.
(Range: 1-65535 seconds)

Default Setting

400 seconds

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ The unsolicited report interval only applies to the interface where MLD proxy has been enabled.
- ◆ MLD and MLD proxy cannot be enabled on the same interface.

Example

The following example sets the interval for sending unsolicited MLD reports to 5 seconds.

```
Console(config)#interface vlan
Console(config-if)#ip igmp proxy unsolicited-report-interval 5
Console(config)#
```

LLDP Commands

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in Type Length Value (TLV) format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) is an extension of LLDP intended for managing endpoint devices such as Voice over IP phones and network switches. The LLDP-MED TLVs advertise information such as network policy, power, inventory, and device location details. LLDP and LLDP-MED information can be used by SNMP applications to simplify troubleshooting, enhance network management, and maintain an accurate network topology.

Table 149: LLDP Commands

Command	Function	Mode
<code>lldp</code>	Enables LLDP globally on the switch	GC
<code>lldp holdtime-multiplier</code>	Configures the time-to-live (TTL) value sent in LLDP advertisements	GC
<code>lldp med-fast-start-count</code>	Configures how many medFastStart packets are transmitted	GC
<code>lldp notification-interval</code>	Configures the allowed interval for sending SNMP notifications about LLDP changes	GC
<code>lldp refresh-interval</code>	Configures the periodic transmit interval for LLDP advertisements	GC
<code>lldp reinit-delay</code>	Configures the delay before attempting to re-initialize after LLDP ports are disabled or the link goes down	GC
<code>lldp tx-delay</code>	Configures a delay between the successive transmission of advertisements initiated by a change in local LLDP MIB variables	GC
<code>lldp admin-status</code>	Enables LLDP transmit, receive, or transmit and receive mode on the specified port	IC
<code>lldp basic-tlv management-ip-address</code>	Configures an LLDP-enabled port to advertise the management address for this device	IC
<code>lldp basic-tlv port-description</code>	Configures an LLDP-enabled port to advertise its port description	IC
<code>lldp basic-tlv system-capabilities</code>	Configures an LLDP-enabled port to advertise its system capabilities	IC

Table 149: LLDP Commands (Continued)

Command	Function	Mode
<code>lldp basic-tlv system-description</code>	Configures an LLDP-enabled port to advertise the system description	IC
<code>lldp basic-tlv system-name</code>	Configures an LLDP-enabled port to advertise its system name	IC
<code>lldp dcbx-tlv ets-config</code>	Configures an LLDP-enabled port to advertise ETS configuration settings	IC
<code>lldp dcbx-tlv ets-recommend</code>	Configures an LLDP-enabled port to advertise ETS recommendation information	IC
<code>lldp dcbx-tlv pfc-config</code>	Configures an LLDP-enabled port to advertise PFC configuration settings	IC
<code>lldp dot1-tlv proto-ident*</code>	Configures an LLDP-enabled port to advertise the supported protocols	IC
<code>lldp dot1-tlv proto-vid*</code>	Configures an LLDP-enabled port to advertise port-based protocol related VLAN information	IC
<code>lldp dot1-tlv pvid*</code>	Configures an LLDP-enabled port to advertise its default VLAN ID	IC
<code>lldp dot1-tlv vlan-name*</code>	Configures an LLDP-enabled port to advertise its VLAN name	IC
<code>lldp dot3-tlv link-agg</code>	Configures an LLDP-enabled port to advertise its link aggregation capabilities	IC
<code>lldp dot3-tlv mac-phy</code>	Configures an LLDP-enabled port to advertise its MAC and physical layer specifications	IC
<code>lldp dot3-tlv max-frame</code>	Configures an LLDP-enabled port to advertise its maximum frame size	IC
<code>lldp med-location civic-addr</code>	Configures an LLDP-MED-enabled port to advertise its location identification details	IC
<code>lldp med-notification</code>	Enables the transmission of SNMP trap notifications about LLDP-MED changes	IC
<code>lldp med-tlv inventory</code>	Configures an LLDP-MED-enabled port to advertise its inventory identification details	IC
<code>lldp med-tlv location</code>	Configures an LLDP-MED-enabled port to advertise its location identification details	IC
<code>lldp med-tlv med-cap</code>	Configures an LLDP-MED-enabled port to advertise its Media Endpoint Device capabilities	IC
<code>lldp med-tlv network-policy</code>	Configures an LLDP-MED-enabled port to advertise its network policy configuration	IC
<code>lldp notification</code>	Enables the transmission of SNMP trap notifications about LLDP changes	IC
<code>show lldp config</code>	Shows LLDP configuration settings for all ports	PE
<code>show lldp info local-device</code>	Shows LLDP global and interface-specific configuration settings for this device	PE

Table 149: LLDP Commands (Continued)

Command	Function	Mode
<code>show lldp info remote-device</code>	Shows LLDP global and interface-specific configuration settings for remote devices	PE
<code>show lldp info statistics</code>	Shows statistical counters for all LLDP-enabled interfaces	PE

* Vendor-specific options may or may not be advertised by neighboring devices.

lldp This command enables LLDP globally on the switch. Use the **no** form to disable LLDP.

Syntax

[no] lldp

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#lldp
Console(config)#
```

lldp holdtime-multiplier This command configures the time-to-live (TTL) value sent in LLDP advertisements. Use the **no** form to restore the default setting.

Syntax

lldp holdtime-multiplier *value*

no lldp holdtime-multiplier

value - Calculates the TTL in seconds based on the following rule:
minimum of ((Transmission Interval * Holdtime Multiplier), or 65536)

(Range: 2 - 10)

Default Setting

Holdtime multiplier: 4

TTL: 4*30 = 120 seconds

Command Mode

Global Configuration

Command Usage

The time-to-live tells the receiving LLDP agent how long to retain all information pertaining to the sending LLDP agent if it does not transmit updates in a timely manner.

Example

```
Console(config)#lldp holdtime-multiplier 10
Console(config)#
```

lldp med-fast-start-count This command specifies the amount of MED Fast Start LLDPDUs to transmit during the activation process of the LLDP-MED Fast Start mechanism.

Syntax

lldp med-fast-start-count *packets*

seconds - Amount of packets. (Range: 1-10 packets; Default: 4 packets)

Default Setting

4 packets

Command Mode

Global Configuration

Command Usage

This parameter is part of the timer which ensures that the LLDP-MED Fast Start mechanism is active for the port. LLDP-MED Fast Start is critical to the timely startup of LLDP, and therefore integral to the rapid availability of Emergency Call Service.

Example

```
Console(config)#lldp med-fast-start-count 6
Console(config)#
```

lldp notification-interval This command configures the allowed interval for sending SNMP notifications about LLDP MIB changes. Use the **no** form to restore the default setting.

Syntax

lldp notification-interval *seconds*

no lldp notification-interval

seconds - Specifies the periodic interval at which SNMP notifications are sent. (Range: 5 - 3600 seconds)

Default Setting

5 seconds

Command Mode

Global Configuration

Command Usage

- ◆ This parameter only applies to SNMP applications which use data stored in the LLDP MIB for network monitoring or management.
- ◆ Information about changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a notification are included in the transmission. An SNMP agent should therefore periodically check the value of `lldpStatsRemTableLastChangeTime` to detect any `lldpRemTablesChange` notification-events missed due to throttling or transmission loss.

Example

```
Console(config)#lldp notification-interval 30
Console(config)#
```

lldp refresh-interval This command configures the periodic transmit interval for LLDP advertisements. Use the **no** form to restore the default setting.

Syntax**lldp refresh-interval** *seconds***no lldp refresh-delay**

seconds - Specifies the periodic interval at which LLDP advertisements are sent. (Range: 5 - 32768 seconds)

Default Setting

30 seconds

Command Mode

Global Configuration

Example

```
Console(config)#lldp refresh-interval 60
Console(config)#
```

lldp reinit-delay This command configures the delay before attempting to re-initialize after LLDP ports are disabled or the link goes down. Use the **no** form to restore the default setting.

Syntax

lldp reinit-delay *seconds*

no lldp reinit-delay

seconds - Specifies the delay before attempting to re-initialize LLDP.
(Range: 1 - 10 seconds)

Default Setting

2 seconds

Command Mode

Global Configuration

Command Usage

When LLDP is re-initialized on a port, all information in the remote systems LLDP MIB associated with this port is deleted.

Example

```
Console(config)#lldp reinit-delay 10
Console(config)#
```

lldp tx-delay This command configures a delay between the successive transmission of advertisements initiated by a change in local LLDP MIB variables. Use the **no** form to restore the default setting.

Syntax

lldp tx-delay *seconds*

no lldp tx-delay

seconds - Specifies the transmit delay. (Range: 1 - 8192 seconds)

Default Setting

2 seconds

Command Mode

Global Configuration

Command Usage

- ◆ The transmit delay is used to prevent a series of successive LLDP transmissions during a short period of rapid changes in local LLDP MIB objects, and to increase the probability that multiple, rather than single changes, are reported in each transmission.

- ◆ This attribute must comply with the following rule:
 $(4 * \text{tx-delay}) \leq \text{refresh-interval}$

Example

```
Console(config)#lldp tx-delay 10
Console(config)#
```

lldp admin-status This command enables LLDP transmit, receive, or transmit and receive mode on the specified port. Use the **no** form to disable this feature.

Syntax

lldp admin-status {rx-only | tx-only | tx-rx}

no lldp admin-status

rx-only - Only receive LLDP PDUs.

tx-only - Only transmit LLDP PDUs.

tx-rx - Both transmit and receive LLDP Protocol Data Units (PDUs).

Default Setting

tx-rx

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp admin-status rx-only
Console(config-if)#
```

lldp basic-tlv management-ip-address This command configures an LLDP-enabled port to advertise the management address for this device. Use the **no** form to disable this feature.

Syntax

[no] lldp basic-tlv management-ip-address

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.
- ◆ The management address TLV may also include information about the specific interface associated with this address, and an object identifier indicating the type of hardware component or protocol entity associated with this address. The interface number and OID are included to assist SNMP applications to perform network discovery by indicating enterprise specific or other starting points for the search, such as the Interface or Entity MIB.
- ◆ Since there are typically a number of different addresses associated with a Layer 3 device, an individual LLDP PDU may contain more than one management address TLV.
- ◆ Every management address TLV that reports an address that is accessible on a port and protocol VLAN through the particular port should be accompanied by a port and protocol VLAN TLV that indicates the VLAN identifier (VID) associated with the management address reported by this TLV.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv management-ip-address
Console(config-if)#
```

lldp basic-tlv port-description This command configures an LLDP-enabled port to advertise its port description. Use the **no** form to disable this feature.

Syntax

[no] lldp basic-tlv port-description

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

The port description is taken from the ifDescr object in RFC 2863, which includes information about the manufacturer, the product name, and the version of the interface hardware/software.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv port-description
Console(config-if)#
```

lldp basic-tlv system-capabilities This command configures an LLDP-enabled port to advertise its system capabilities. Use the **no** form to disable this feature.

Syntax

[no] lldp basic-tlv system-capabilities

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

The system capabilities identifies the primary function(s) of the system and whether or not these primary functions are enabled. The information advertised by this TLV is described in IEEE 802.1AB.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-capabilities
Console(config-if)#
```

lldp basic-tlv system-description This command configures an LLDP-enabled port to advertise the system description. Use the **no** form to disable this feature.

Syntax

[no] lldp basic-tlv system-description

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

The system description is taken from the sysDescr object in RFC 3418, which includes the full name and version identification of the system's hardware type, software operating system, and networking software.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-description
Console(config-if)#
```

lldp basic-tlv system-name This command configures an LLDP-enabled port to advertise the system name. Use the **no** form to disable this feature.

Syntax

[no] lldp basic-tlv system-name

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

The system name is taken from the sysName object in RFC 3418, which contains the system's administratively assigned name, and is in turn based on the [hostname](#) command.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-name
Console(config-if)#
```

lldp dcbx-tlv ets-config This command configures an LLDP-enabled port to advertise ETS configuration settings. Use the **no** form to disable this feature.

Syntax

[no] lldp dcbx-tlv ets-config

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ This command will take effect when DCBX is enabled (using the [dcbx](#) command).

- ◆ If you configure ETS on an interface (using the [ets mode](#) command), DCBX advertises each priority group on the interface, the priorities in each priority group, and the bandwidth properties of each priority group and priority.
- ◆ If you do not configure ETS on an interface, DCBX advertises the default priority group, its priorities, and the assigned bandwidth.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp dcbx-tlv ets-config
Console(config-if)#
```

lldp dcbx-tlv ets-recommend

This command configures an LLDP-enabled port to advertise the ETS settings that the switch wants the connected peer interface to use. Use the **no** form to disable this feature.

Syntax

[no] lldp dcbx-tlv ets-recommend

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ If the peer interface is “willing,” it changes its configuration to match the configuration in the ETS Recommendation TLV.
- ◆ If you disable the ETS Recommendation TLV, the switch still sends the ETS Configuration TLV to the connected peer. The connected peer is informed about the switch DCBX ETS configuration, but even if the peer is “willing,” the peer does not change its configuration to match the switch configuration.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp dcbx-tlv ets-recommend
Console(config-if)#
```

lldp dcbx-tlv pfc-config This command configures an LLDP-enabled port to advertise PFC configuration settings. Use the **no** form to disable this feature.

Syntax

[no] lldp dcbx-tlv pfc-config

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ After enabling PFC on a switch interface (using the [pfc mode](#) command), DCBX uses autonegotiation to control the operational state of the PFC functionality.
- ◆ If the peer is “willing” to learn its PFC configuration from the switch, DCBX pushes the switch’s PFC configuration to the peer.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp dcbx-tlv pfc-config
Console(config-if)#
```

lldp dot1-tlv proto-ident This command configures an LLDP-enabled port to advertise the supported protocols. Use the **no** form to disable this feature.

Syntax

[no] lldp dot1-tlv proto-ident

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This option advertises the protocols that are accessible through this interface.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv proto-ident
Console(config-if)#
```

lldp dot1-tlv proto-vid This command configures an LLDP-enabled port to advertise port-based protocol VLAN information. Use the **no** form to disable this feature.

Syntax

[no] lldp dot1-tlv proto-vid

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This option advertises the port-based protocol VLANs configured on this interface (see [“Configuring Protocol-based VLANs” on page 512](#)).

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv proto-vid
Console(config-if)#
```

lldp dot1-tlv pvid This command configures an LLDP-enabled port to advertise its default VLAN ID. Use the **no** form to disable this feature.

Syntax

[no] lldp dot1-tlv pvid

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

The port's default VLAN identifier (PVID) indicates the VLAN with which untagged or priority-tagged frames are associated (see the [switchport native vlan](#) command).

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv pvid
Console(config-if)#
```

lldp dot1-tlv vlan-name This command configures an LLDP-enabled port to advertise its VLAN name. Use the **no** form to disable this feature.

Syntax

[no] lldp dot1-tlv vlan-name

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This option advertises the name of all VLANs to which this interface has been assigned. See [switchport allowed vlan](#) and [protocol-vlan protocol-group \(Configuring Interfaces\)](#).

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv vlan-name
Console(config-if)#
```

lldp dot3-tlv link-agg This command configures an LLDP-enabled port to advertise link aggregation capabilities. Use the **no** form to disable this feature.

Syntax

[no] lldp dot3-tlv link-agg

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This option advertises link aggregation capabilities, aggregation status of the link, and the 802.3 aggregated port identifier if this interface is currently a link aggregation member.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot3-tlv link-agg
Console(config-if)#
```

lldp dot3-tlv mac-phy This command configures an LLDP-enabled port to advertise its MAC and physical layer capabilities. Use the **no** form to disable this feature.

Syntax

[no] lldp dot3-tlv mac-phy

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This option advertises MAC/PHY configuration/status which includes information about auto-negotiation support/capabilities, and operational Multistation Access Unit (MAU) type.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot3-tlv mac-phy
Console(config-if)#
```

lldp dot3-tlv max-frame This command configures an LLDP-enabled port to advertise its maximum frame size. Use the **no** form to disable this feature.

Syntax

[no] lldp dot3-tlv max-frame

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

Refer to [“Frame Size” on page 121](#) for information on configuring the maximum frame size for this switch.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp dot3-tlv max-frame
Console(config-if)#
```

lldp med-location civic-addr This command configures an LLDP-MED-enabled port to advertise its location identification details. Use the **no** form to restore the default settings.

Syntax

lldp med-location civic-addr [[**country** *country-code*] | [**what** *device-type*] | [*ca-type* *ca-value*]]

no lldp med-location civic-addr [[**country**] | [**what**] | [*ca-type*]]

country-code – The two-letter ISO 3166 country code in capital ASCII letters. (Example: DK, DE or US)

device-type – The type of device to which the location applies.

0 – Location of DHCP server.

1 – Location of network element closest to client.

2 – Location of client.

ca-type – A one-octet descriptor of the data civic address value. (Range: 0-255)

ca-value – Description of a location. (Range: 1-32 characters)

Default Setting

Not advertised

No description

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ Use this command without any keywords to advertise location identification details.
- ◆ Use the *ca-type* to advertise the physical location of the device, that is the city, street number, building and room information. The address location is specified as a type and value pair, with the civic address (CA) type being defined in RFC 4776. The following table describes some of the CA type numbers and provides examples.

Table 150: LLDP MED Location CA Types

CA Type	Description	CA Value Example
1	National subdivisions (state, canton, province)	California
2	County, parish	Orange
3	City, township	Irvine
4	City division, borough, city district	West Irvine
5	Neighborhood, block	Riverside

Table 150: LLDP MED Location CA Types (Continued)

CA Type	Description	CA Value Example
6	Group of streets below the neighborhood level	Exchange
18	Street suffix or type	Avenue
19	House number	320
20	House number suffix	A
21	Landmark or vanity address	Tech Center
26	Unit (apartment, suite)	Apt 519
27	Floor	5
28	Room	509B

Any number of CA type and value pairs can be specified for the civic address location, as long as the total does not exceed 250 characters.

- ◆ For the location options defined for *device-type*, normally option **2** is used to specify the location of the client device. In situations where the client device location is not known, **0** and **1** can be used, providing the client device is physically close to the DHCP server or network element.

Example

The following example enables advertising location identification details.

```

Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-location civic-addr
Console(config-if)#lldp med-location civic-addr 1 California
Console(config-if)#lldp med-location civic-addr 2 Orange
Console(config-if)#lldp med-location civic-addr 3 Irvine
Console(config-if)#lldp med-location civic-addr 4 West Irvine
Console(config-if)#lldp med-location civic-addr 6 Exchange
Console(config-if)#lldp med-location civic-addr 18 Avenue
Console(config-if)#lldp med-location civic-addr 19 320
Console(config-if)#lldp med-location civic-addr 27 5
Console(config-if)#lldp med-location civic-addr 28 509B
Console(config-if)#lldp med-location civic-addr country US
Console(config-if)#lldp med-location civic-addr what 2
Console(config-if)#

```

lldp med-notification This command enables the transmission of SNMP trap notifications about LLDP-MED changes. Use the **no** form to disable LLDP-MED notifications.

Syntax

[no] lldp med-notification

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ This option sends out SNMP trap notifications to designated target stations at the interval specified by the `lldp notification-interval` command. Trap notifications include information about state changes in the LLDP MIB (IEEE 802.1AB), the LLDP-MED MIB (ANSI/TIA 1057), or organization-specific LLDP-EXT-DOT1 and LLDP-EXT-DOT3 MIBs.
- ◆ SNMP trap destinations are defined using the `snmp-server host` command.
- ◆ Information about additional changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a trap notification are included in the transmission. An SNMP agent should therefore periodically check the value of `lldpStatsRemTableLastChangeTime` to detect any `lldpRemTablesChange` notification-events missed due to throttling or transmission loss.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-notification
Console(config-if)#
```

lldp med-tlv inventory This command configures an LLDP-MED-enabled port to advertise its inventory identification details. Use the **no** form to disable this feature.

Syntax**[no] lldp med-tlv inventory****Default Setting**

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This option advertises device details useful for inventory management, such as manufacturer, model, software version and other pertinent information.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp med-tlv inventory
Console(config-if)#
```


lldp med-tlv location This command configures an LLDP-MED-enabled port to advertise its location identification details. Use the **no** form to disable this feature.

Syntax

[no] lldp med-tlv location

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This option advertises location identification details.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-tlv location
Console(config-if)#
```

lldp med-tlv med-cap This command configures an LLDP-MED-enabled port to advertise its Media Endpoint Device capabilities. Use the **no** form to disable this feature.

Syntax

[no] lldp med-tlv med-cap

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This option advertises LLDP-MED TLV capabilities, allowing Media Endpoint and Connectivity Devices to efficiently discover which LLDP-MED related TLVs are supported on the switch.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-tlv med-cap
Console(config-if)#
```

lldp med-tlv network-policy This command configures an LLDP-MED-enabled port to advertise its network policy configuration. Use the **no** form to disable this feature.

Syntax

[no] lldp med-tlv network-policy

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This option advertises network policy configuration information, aiding in the discovery and diagnosis of VLAN configuration mismatches on a port. Improper network policy configurations frequently result in voice quality degradation or complete service disruption.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-tlv network-policy
Console(config-if)#
```

lldp notification This command enables the transmission of SNMP trap notifications about LLDP changes. Use the **no** form to disable LLDP notifications.

Syntax

[no] lldp notification

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ This option sends out SNMP trap notifications to designated target stations at the interval specified by the [lldp notification-interval](#) command. Trap notifications include information about state changes in the LLDP MIB (IEEE 802.1AB), or organization-specific LLDP-EXT-DOT1 and LLDP-EXT-DOT3 MIBs.
- ◆ SNMP trap destinations are defined using the [snmp-server host](#) command.
- ◆ Information about additional changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a trap notification are included in the transmission. An SNMP agent should

therefore periodically check the value of `lldpStatsRemTableLastChangeTime` to detect any `lldpRemTablesChange` notification-events missed due to throttling or transmission loss.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp notification
Console(config-if)#
```

show lldp config This command shows LLDP configuration settings for all ports.

Syntax

show lldp config [**detail** *interface*]

detail - Shows configuration summary.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Command Mode

Privileged Exec

Example

```
Console#show lldp config
LLDP Global Configuration
LLDP Enabled : Yes
LLDP Transmit Interval : 30 sec.
LLDP Hold Time Multiplier : 4
LLDP Delay Interval : 2 sec.
LLDP Re-initialization Delay : 2 sec.
LLDP Notification Interval : 5 sec.
LLDP MED Fast Start Count : 4

LLDP Port Configuration
Port Admin Status Notification Enabled
-----
Eth 1/1 Tx-Rx True
Eth 1/2 Tx-Rx True
Eth 1/3 Tx-Rx True
Eth 1/4 Tx-Rx True
Eth 1/5 Tx-Rx True
.
.
.
Console#show lldp config detail ethernet 1/1
LLDP Port Configuration Detail
Port : Eth 1/1
Admin Status : Tx-Rx
Notification Enabled : True
```

```

Basic TLVs Advertised      : port-description
                           : system-name
                           : system-capabilities
                           : management-ip-address
802.1 specific TLVs Advertised : port-vid
                           : vlan-name
                           : proto-vlan
                           : proto-ident
802.3 specific TLVs Advertised : mac-phy
                           : link-agg
                           : max-frame
MED Notification Status    : Enabled
MED Enabled TLVs Advertised : med-cap
                           : network-policy
                           : location
                           : inventory
MED Location Identification:
Location Data Format : Civic Address LCI
Country Name       : US
What               : 2 - DHCP Client
CA Type 1          : California
CA Type 2          : Orange
DCBX specific TLVs Advertised : ets-config
                           : ets-recommend
                           : pfc-config
Console#

```

show lldp info local-device This command shows LLDP global and interface-specific configuration settings for this device.

Syntax

show lldp info local-device [**detail** *interface*]

detail - Shows configuration summary.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Command Mode

Privileged Exec

Example

```

Console#show lldp info local-device
LLDP Local Global Information
Chassis Type           : MAC Address
Chassis ID             : 00-E0-0C-02-00-FD
System Name            :
System Description      : ECS5610-52S
System Capabilities Support : Bridge, Router
System Capabilities Enabled : Bridge, Router
Management Address     : 192.168.0.3 (IPv4)

```

```

LLDP Local Port Information
Port      Port ID Type  Port ID          Port Description
-----
Eth 1/1   MAC Address   00-E0-0C-02-00-FE Ethernet Port on unit 1, port 1
Eth 1/2   MAC Address   00-E0-0C-02-00-FF Ethernet Port on unit 1, port 2
Eth 1/3   MAC Address   00-E0-0C-02-01-00 Ethernet Port on unit 1, port 3
Eth 1/4   MAC Address   00-E0-0C-02-01-01 Ethernet Port on unit 1, port 4
.
.
.
Console#show lldp info local-device detail ethernet 1/1

LLDP Port Information Details

Port          : Eth 1/1
Port Type     : MAC Address
Port ID       : 00-E0-0C-00-00-AE
Port Description : Ethernet Port on unit 0, port 1
MED Capability : LLDP-MED Capabilities
                  Network Policy
                  Location Identification
                  Inventory

Console#

```

show lldp info remote-device This command shows LLDP global and interface-specific configuration settings for remote devices attached to an LLDP-enabled port.

Syntax

show lldp info remote-device [**detail** *interface*]

detail - Shows configuration summary.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Command Mode

Privileged Exec

Example

Note that an IP phone or other end-node device which advertises LLDP-MED capabilities must be connected to the switch for information to be displayed in the "Device Class" field.

```

Console#show lldp info remote-device

LLDP Remote Devices Information

Interface Chassis ID          Port ID          System Name
-----
Eth 1/1   00-E0-0C-00-00-FD 00-E0-0C-00-01-02

```

```
Console#show lldp info remote-device detail ethernet 1/1
```

```
-----
Local Port Name      : Eth 1/1
Chassis Type         : MAC Address
Chassis ID           : 00-01-02-03-04-05
Port ID Type         : Network Address
Port ID              : 00-01-02-03-04-06
System Name          :
System Description   :
System Description   : ECS5110-12M
SystemCapSupported   : Bridge
SystemCapEnabled     : Bridge
Remote Management Address :
    192.168.1.2 (IPv4)
Remote Port VID      : 1
Remote Port-Protocol VLAN :
    VLAN-3 : supported, enabled
Remote VLAN Name     :
    VLAN-1 : DefaultVlan
Remote Protocol Identity (Hex) :
    88-CC
Remote MAC/PHY Configuration Status :
    Remote port auto-neg supported : Yes
    Remote port auto-neg enabled : Yes
    Remote port auto-neg advertised cap (Hex) : 0000
    Remote port MAU type : 6
Remote Power via MDI :
    Remote power class : PSE
    Remote power MDI supported : Yes
    Remote power MDI enabled : Yes
    Remote power pair controllable : No
    Remote power pairs : Spare
    Remote power classification : Class1
Remote Link Aggregation :
    Remote link aggregation capable : Yes
    Remote link aggregation enable : No
    Remote link aggregation port ID : 0
Remote Max Frame Size : 1518
LLDP-MED Capability :
    Device Class : Network Connectivity
    Supported Capabilities : LLDP-MED Capabilities
                             Network Policy
                             Location Identification
                             Extended Power via MDI - PSE
                             Inventory
    Current Capabilities : LLDP-MED Capabilities
                             Location Identification
                             Extended Power via MDI - PSE
                             Inventory
Location Identification :
    Location Data Format : Civic Address LCI
    Country Name : TW
    What : 2
Extended Power via MDI :
    Power Type : PSE
    Power Source : Unknown
    Power Priority : Unknown
    Power Value : 0 Watts
Inventory :
    Hardware Revision : R01
    Firmware Revision : 1.2.2.1
    Software Revision : 1.2.2.1
    Serial Number :
    Manufacture Name :
    Model Name :
```

```

Asset ID                               :
Console#

```

show lldp info statistics This command shows statistics based on traffic received through all attached LLDP-enabled interfaces.

Syntax

show lldp info statistics [**detail** *interface*]

detail - Shows configuration summary.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Command Mode

Privileged Exec

Example

```

Console#show lldp info statistics

LLDP Device Statistics

Neighbor Entries List Last Updated : 2450279 seconds
New Neighbor Entries Count         : 1
Neighbor Entries Deleted Count     : 0
Neighbor Entries Dropped Count     : 0
Neighbor Entries Ageout Count      : 0

Port      NumFramesRecvd  NumFramesSent  NumFramesDiscarded
-----
Eth 1/1   0                83             0
Eth 1/2   11               12             0
Eth 1/3   0                0              0
Eth 1/4   0                0              0
Eth 1/5   0                0              0
:
Console#show lldp info statistics detail ethernet 1/1
LLDP Port Statistics Detail
Port Name      : Eth 1/1
Frames Discarded : 0
Frames Invalid  : 0
Frames Received : 327
Frames Sent     : 328
TLVs Unrecognized : 0
TLVs Discarded  : 0
Neighbor Ageouts : 0

Console#

```


Domain Name Service Commands

These commands are used to configure Domain Naming System (DNS) services. Entries can be manually configured in the DNS domain name to IP address mapping table, default domain names configured, or one or more name servers specified to use for domain name to address translation.

Note that domain name services will not be enabled until at least one name server is specified with the `ip name-server` command and domain lookup is enabled with the `ip domain-lookup` command.

Table 151: Address Table Commands

Command	Function	Mode
<code>ip domain-list</code>	Defines a list of default domain names for incomplete host names	GC
<code>ip domain-lookup</code>	Enables DNS-based host name-to-address translation	GC
<code>ip domain-name</code>	Defines a default domain name for incomplete host names	GC
<code>ip host</code>	Creates a static IPv4 host name-to-address mapping	GC
<code>ip name-server</code>	Specifies the address of one or more name servers to use for host name-to-address translation	GC
<code>ipv6 host</code>	Creates a static IPv6 host name-to-address mapping	GC
<code>clear dns cache</code>	Clears all entries from the DNS cache	PE
<code>clear host</code>	Deletes entries from the host name-to-address table	PE
<code>show dns</code>	Displays the configuration for DNS services	PE
<code>show dns cache</code>	Displays entries in the DNS cache	PE
<code>show hosts</code>	Displays the static host name-to-address mapping table	PE

ip domain-list This command defines a list of domain names that can be appended to incomplete host names (i.e., host names passed from a client that are not formatted with dotted notation). Use the **no** form to remove a name from this list.

Syntax

[no] ip domain-list *name*

name - Name of the host. Do not include the initial dot that separates the host name from the domain name. (Range: 1-127 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ Domain names are added to the end of the list one at a time.
- ◆ When an incomplete host name is received by the DNS service on this switch, it will work through the domain list, appending each domain name in the list to the host name, and checking with the specified name servers for a match.
- ◆ If there is no domain list, the domain name specified with the [ip domain-name](#) command is used. If there is a domain list, the default domain name is not used.

Example

This example adds two domain names to the current list and then displays the list.

```

Console(config)#ip domain-list sample.com.jp
Console(config)#ip domain-list sample.com.uk
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS Disabled
Default Domain Name:
    sample.com
Domain Name List:
    sample.com.jp
    sample.com.uk
Name Server List:
Console#

```

Related Commands

[ip domain-name \(723\)](#)

ip domain-lookup This command enables DNS host name-to-address translation. Use the **no** form to disable DNS.

Syntax

[no] ip domain-lookup

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ At least one name server must be specified before DNS can be enabled.
- ◆ If all name servers are deleted, DNS will automatically be disabled.

Example

This example enables DNS and then displays the configuration.

```

Console(config)#ip domain-lookup
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS Enabled
Default Domain Name:
    sample.com
Domain Name List:
    sample.com.jp
    sample.com.uk
Name Server List:
    192.168.1.55
    10.1.0.55
Console#

```

Related Commands

[ip domain-name \(723\)](#)

[ip name-server \(724\)](#)

ip domain-name This command defines the default domain name appended to incomplete host names (i.e., host names passed from a client that are not formatted with dotted notation). Use the **no** form to remove the current domain name.

Syntax

ip domain-name *name*

no ip domain-name

name - Name of the host. Do not include the initial dot that separates the host name from the domain name.
(Range: 1-127 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```

Console(config)#ip domain-name sample.com
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS Disabled
Default Domain Name:
    sample.com
Domain Name List:
Name Server List:
Console#

```

Related Commands

[ip domain-list \(721\)](#)
[ip name-server \(724\)](#)
[ip domain-lookup \(722\)](#)

ip host This command creates a static entry in the DNS table that maps a host name to an IPv4 address. Use the **no** form to remove an entry.

Syntax

[no] ip host *name address*

name - Name of an IPv4 host. (Range: 1-100 characters)

address - Corresponding IPv4 address.

Default Setting

No static entries

Command Mode

Global Configuration

Command Usage

Use the **no ip host** command to clear static entries, or the [clear host](#) command to clear dynamic entries.

Example

This example maps an IPv4 address to a host name.

```

Console(config)#ip host rd5 192.168.1.55
Console(config)#end
Console#show hosts
No.  Flag Type      IP Address          TTL    Domain
-----
0    2 Address 192.168.1.55          rd5
Console#

```

ip name-server This command specifies the address of one or more domain name servers to use for name-to-address resolution. Use the **no** form to remove a name server from this list.

Syntax

[no] ip name-server *server-address1* [*server-address2* ...
server-address6]

server-address1 - IPv4 or IPv6 address of domain-name server.

server-address2 ... *server-address6* - IPv4 or IPv6 address of additional domain-name servers.

Default Setting

None

Command Mode

Global Configuration

Command Usage

The listed name servers are queried in the specified sequence until a response is received, or the end of the list is reached with no response.

Example

This example adds two domain-name servers to the list and then displays the list.

```

Console(config)#ip name-server 192.168.1.55 10.1.0.55
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS disabled
Default Domain Name:
    sample.com
Domain Name List:
    sample.com.jp
    sample.com.uk
Name Server List:
    192.168.1.55
    10.1.0.55
Console#

```

Related Commands

[ip domain-name \(723\)](#)

[ip domain-lookup \(722\)](#)

ipv6 host This command creates a static entry in the DNS table that maps a host name to an IPv6 address. Use the **no** form to remove an entry.

Syntax

[no] ipv6 host *name ipv6-address*

name - Name of an IPv6 host. (Range: 1-100 characters)

ipv6-address - Corresponding IPv6 address. This address must be entered according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

Default Setting

No static entries

Command Mode

Global Configuration

Example

This example maps an IPv6 address to a host name.

```

Console(config)#ipv6 host rd6 2001:0db8:1::12
Console(config)#end
Console#show hosts

```

No.	Flag	Type	IP Address	TTL	Domain
0	2	Address	192.168.1.55		rd5
1	2	Address	2001:DB8:1::12		rd6

```

Console#

```

clear dns cache This command clears all entries in the DNS cache.**Command Mode**

Privileged Exec

Example

```

Console#clear dns cache
Console#show dns cache

```

No.	Flag	Type	IP Address	TTL	Domain
-----	------	------	------------	-----	--------

```

Console#

```

clear host This command deletes dynamic entries from the DNS table.**Syntax****clear host** {*name* | *}
name - Name of the host. (Range: 1-100 characters)

* - Removes all entries.

Default Setting

None

Command Mode

Privileged Exec

Command UsageUse the **clear host** command to clear dynamic entries, or the **no ip host** command to clear static entries.

Example

This example clears all dynamic entries from the DNS table.

```
Console(config)#clear host *
Console(config)#
```

show dns This command displays the configuration of the DNS service.

Command Mode

Privileged Exec

Example

```
Console#show dns
Domain Lookup Status:
  DNS enabled
Default Domain Name:
  sample.com
Domain Name List:
  sample.com.jp
  sample.com.uk
Name Server List:
  192.168.1.55
  10.1.0.55
Console#
```

show dns cache This command displays entries in the DNS cache.

Command Mode

Privileged Exec

Example

```
Console#show dns cache
No.      Flag    Type    IP Address    TTL    Host
-----
      3      4 Host    209.131.36.158  115    www-real.wal.b.yahoo.com
      4      4 CNAME    POINTER TO:3    115    www.yahoo.com
      5      4 CNAME    POINTER TO:3    115    www.wal.b.yahoo.com
Console#
```

Table 152: show dns cache - display description

Field	Description
No.	The entry number for each resource record.
Flag	The flag is always "4" indicating a cache entry and therefore unreliable.
Type	This field includes "Host" which specifies the primary name for the owner, and "CNAME" which specifies multiple domain names (or aliases) which are mapped to the same IP address as an existing entry.

Table 152: show dns cache - display description (Continued)

Field	Description
IP Address	The IP address associated with this record.
TTL	The time to live reported by the name server.
Host	The host name associated with this record.

show hosts This command displays the static host name-to-address mapping table.

Command Mode

Privileged Exec

Example

Note that a host name will be displayed as an alias if it is mapped to the same address(es) as a previously configured entry.

```

Console#show hosts
No.  Flag Type      IP Address          TTL  Domain
-----
0    2  Address 192.168.1.55          rd5
1    2  Address 2001:DB8:1::12       rd6
3    4  Address 209.131.36.158       65 www-real.wa1.b.yahoo.com
4    4  CNAME   POINTER TO:3         65 www.yahoo.com
5    4  CNAME   POINTER TO:3         65 www.wa1.b.yahoo.com
Console#

```

Table 153: show hosts - display description

Field	Description
No.	The entry number for each resource record.
Flag	The field displays "2" for a static entry, or "4" for a dynamic entry stored in the cache.
Type	This field includes "Address" which specifies the primary name for the owner, and "CNAME" which specifies multiple domain names (or aliases) which are mapped to the same IP address as an existing entry.
IP Address	The IP address associated with this record.
TTL	The time to live reported by the name server. This field is always blank for static entries.
Domain	The domain name associated with this record.

DHCP Commands

These commands are used to configure Dynamic Host Configuration Protocol (DHCP) client, relay, and server functions. Any VLAN interface can be configured to automatically obtain an IPv4 address through DHCP. This switch can be configured to relay DHCP client configuration requests to a DHCP server on another network, or it can be configured to provide DHCP service directly to any client.

Table 154: DHCP Commands

Command Group	Function
DHCP Client	Allows interfaces to dynamically acquire IPv4 address information
DHCP Relay	Relays DHCP requests from local hosts to a remote DHCP server
DHCP Server	Configures DHCP service using address pools or static bindings

DHCP Client

Use the commands in this section to allow the switch's VLAN interfaces to dynamically acquire IP address information.

Table 155: DHCP Client Commands

Command	Function	Mode
<i>DHCP for IPv4</i>		
<code>ip dhcp client class-id</code>	Specifies the DHCP client identifier for an interface	IC
<code>ip dhcp restart client</code>	Submits a BOOTP or DHCP client request	PE
<i>DHCP for IPv6</i>		
<code>ipv6 dhcp client rapid-commit vlan</code>	Specifies the Rapid Commit option for DHCPv6 message exchange	GC

ip dhcp client class-id This command specifies the DHCP client vendor class identifier for the current interface. Use the **no** form to remove the class identifier from the DHCP packet.

Syntax

ip dhcp client class-id [`text text` | `hex hex`]

no ip dhcp client class-id

text - A text string. (Range: 1-32 characters)

hex - A hexadecimal value. (Range: 1-64 characters)

Default Setting

Class identifier option enabled, with the name ECS5610-52S

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ Use this command without any keyword to restore the default setting.
- ◆ This command is used to identify the vendor class and configuration of the switch to the DHCP server, which then uses this information to decide on how to service the client or the type of information to return.
- ◆ The general framework for this DHCP option is set out in RFC 2132 (Option 60). This information is used to convey configuration settings or other identification information about a client, but the specific string to use should be supplied by your service provider or network administrator. Options 60, 66 and 67 statements can be added to the server daemon's configuration file.

Table 156: Options 60, 66 and 67 Statements

Option	Statement	
	Keyword	Parameter
60	vendor-class-identifier	a string indicating the vendor class identifier
66	tftp-server-name	a string indicating the tftp server name
67	bootfile-name	a string indicating the bootfile name

- ◆ By default, DHCP option 66/67 parameters are not carried in a DHCP server reply. To ask for a DHCP reply with option 66/67 information, the DHCP client request sent by this switch includes a "parameter request list" asking for this information. Besides, the client request also includes a "vendor class identifier" that allows the DHCP server to identify the device, and select the appropriate configuration file for download. This information is included in Option 55 and 124.

Table 157: Options 55 and 124 Statements

Option	Statement	
	Keyword	Parameter
55	dhcp-parameter-request-list	a list of parameters, separated by "
124	vendor-class-identifier	a string indicating the vendor class identifier

- ◆ The server should reply with the TFTP server name and boot file name.

- ◆ Note that the vendor class identifier can be formatted in either text or hexadecimal, but the format used by both the client and server must be the same.

Example

```
Console(config)#interface vlan 2
Console(config-if)#ip dhcp client class-id hex 0000e8666572
Console(config-if)#
```

Related Commands

[ip dhcp restart client \(731\)](#)

ip dhcp restart client This command submits a BOOTP or DHCP client request.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- ◆ This command issues a BOOTP or DHCP client request for any IP interface that has been set to BOOTP or DHCP mode through the [ip address](#) command.
- ◆ DHCP requires the server to reassign the client's last address if available.
- ◆ If the BOOTP or DHCP server has been moved to a different domain, the network portion of the address provided to the client will be based on this new domain.

Example

In the following example, the device is reassigned the same address.

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#exit
Console#ip dhcp restart client
Console#show ip interface
VLAN 1 is Administrative Up - Link Up
  Address is 12-34-12-34-12-34
  Index: 1001, MTU: 1500
  Address Mode is DHCP
  IP Address: 192.168.0.9 Mask: 255.255.255.0
  Proxy ARP is disabled
Console#
```

Related Commands

[ip address \(750\)](#)

ipv6 dhcp client rapid-commit vlan This command specifies the Rapid Commit option for DHCPv6 message exchange for all DHCPv6 client requests submitted from the specified interface. Use the **no** form to disable this option.

Syntax

[no] ipv6 dhcp client rapid-commit vlan *vlan-list*

vlan-list - VLAN ID, specified as a single number, a range of consecutive numbers separated by a hyphen, or multiple numbers separated by commas. (Range: 1-4094; Maximum command length: 300 characters)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ DHCPv6 clients can obtain configuration parameters from a server through a normal four-message exchange (solicit, advertise, request, reply), or through a rapid two-message exchange (solicit, reply). The rapid-commit option must be enabled on both client and server for the two-message exchange to be used.
- ◆ This command allows two-message exchange method for prefix delegation. When enabled, DHCPv6 client requests submitted from the specified interface will include the rapid commit option in all solicit messages.
- ◆ If the rapid commit option has been enabled on the switch using the **ipv6 dhcp client rapid-commit vlan** command, and on the DHCPv6 server, message exchange can be reduced from the normal four step process to a two-step exchange of only solicit and reply messages.

Example

```
ES-3026(config)#ipv6 dhcp client rapid-commit vlan 2
ES-3026(config)#
```

DHCP Relay

This section describes commands used to configure DHCP relay functions for host devices attached to the switch.

Table 158: DHCP Relay Commands

Command	Function	Mode
<i>DHCP for IPv4</i>		
<code>ip dhcp relay server</code>	Specifies DHCP server addresses for relay	IC
<code>ip dhcp restart relay</code>	Enables DHCP relay agent	PE
<i>DHCP for IPv6</i>		
<code>ipv6 dhcp relay destination</code>	Specifies a DHCPv6 server or VLAN to which client requests are forwarded and enables DHCPv6 relay service	IC
<code>show ipv6 dhcp relay destination</code>	Displays a DHCPv6 server or VLAN to which client requests are forwarded	PE

DHCP for IPv4

ip dhcp relay server This command specifies the addresses of DHCP servers to be used by the switch's DHCP relay agent. Use the **no** form to clear all addresses.

Syntax

ip dhcp relay server *address1* [*address2* [*address3* ...]]

no ip dhcp relay server

address - IP address of DHCP server. (Range: 1-3 addresses)

Default Setting

None

Command Mode

Interface Configuration (VLAN)

Usage Guidelines

- ◆ You must specify the IP address for at least one DHCP server. Otherwise, the switch's DHCP relay agent will not forward client requests to a DHCP server.
- ◆ To start DHCP relay service, enter the `ip dhcp restart relay` command.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip dhcp relay server 10.1.0.99
Console(config-if)#
```

Related Commands

[ip dhcp restart relay \(734\)](#)

ip dhcp restart relay This command enables DHCP relay for the specified VLAN. Use the **no** form to disable it.

Syntax

ip dhcp restart relay

Default Setting

Disabled

Command Mode

Privileged Exec

Command Usage

This command is used to configure DHCP relay functions for host devices attached to the switch. If DHCP relay service is enabled, and this switch sees a DHCP request broadcast, it inserts its own IP address into the request so the DHCP server will know the subnet where the client is located. Then, the switch forwards the packet to the DHCP server on another network. When the server receives the DHCP request, it allocates a free IP address for the DHCP client from its defined scope for the DHCP client's subnet, and sends a DHCP response back to the DHCP relay agent (i.e., this switch). This switch then broadcasts the DHCP response received from the server to the client.

Example

In the following example, the device is reassigned the same address.

```
Console(config)#ip dhcp restart relay
Console(config)#end
Console#show ip interface
VLAN 1 is Administrative Up - Link Up
  Address is 00-00-0C-00-00-FD
  Index: 1001, MTU: 1500
  Address Mode is DHCP
  IP Address: 192.168.0.3 Mask: 255.255.255.0
  Proxy ARP is disabled
Console#
```

Related Commands

[ip dhcp relay server \(733\)](#)

DHCP for IPv6

ipv6 dhcp relay destination This command specifies a DHCPv6 server or the VLAN to which client requests are forwarded, and also enables DHCPv6 relay service on this interface. Use the **no** form to disable this service.

Syntax

ipv6 dhcp relay destination {*ipv6-address* | **multicast** {**all** | **vlan** *vlan-id*}}

no ipv6 dhcp relay destination [*ipv6-address* | **multicast** {**all** | **vlan** *vlan-id*}]

ipv6-address - IPv6 address of a DHCPv6 server or another relay server.
(Range: 1-3 addresses)

multicast - Uses the all DHCPv6 server multicast address.

all - Specifies all local VLAN interfaces.

vlan-id - VLAN ID (Range: 1-4094)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- ◆ You must specify the IPv6 address for at least one DHCPv6 server or another relay agent, or the VLAN to which to multicast a relay message. Otherwise, the switch's DHCPv6 relay agent will not forward client requests. This command enables DHCPv6 relay service for the VLAN from which the command is entered.
- ◆ Up to five destination addresses may be defined using consecutive commands.
- ◆ This command is used to configure DHCPv6 relay functions for host devices attached to the switch. If DHCPv6 relay service is enabled (by entering this command), and this switch sees a DHCPv6 request broadcast, it inserts its own IPv6 address into the request so the DHCPv6 server will know the subnet where the client is located. Then, the switch forwards the packet to the DHCPv6 server on another network. When the server receives the DHCPv6 request, it allocates a free IPv6 address for the DHCPv6 client from its defined scope for the DHCPv6 client's subnet, and sends a DHCPv6 response back to the DHCPv6 relay agent (i.e., this switch). This switch then broadcasts the DHCPv6 response received from the server to the client.

Example

In the following example, the device is reassigned the same address.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 dhcp relay destination multicast vlan 2
Console(config-if)#
Console#
```

show ipv6 dhcp relay destination This command displays a DHCPv6 server or the VLAN to which client requests are forwarded.

Syntax

show ipv6 dhcp relay destination interface [vlan *vlan-id*]

vlan-id - VLAN ID (Range: 1-4094)

Command Mode

Privileged Exec

Example

```
Console#show ipv6 dhcp relay destination interface vlan 1
DHCP relay destination :
VLAN 1 :
    Multicast : VLAN 2
Console#
```

DHCP Server

This section describes commands used to configure client address pools for the DHCP service.

Table 159: DHCP Server Commands

Command	Function	Mode
ip dhcp excluded-address	Specifies IP addresses that a DHCP server should not assign to DHCP clients	GC
ip dhcp pool	Configures a DHCP address pool on a DHCP Server	GC
service dhcp	Enables the DHCP server feature on this switch	GC
bootfile	Specifies a default boot image for a DHCP client	DC
client-identifier*	Specifies a client identifier for a DHCP client	DC
default-router	Specifies the default router list for a DHCP client	DC
dns-server	Specifies the Domain Name Server (DNS) servers available to a DHCP client	DC
domain-name	Specifies the domain name for a DHCP client	DC

Table 159: DHCP Server Commands (Continued)

Command	Function	Mode
<code>hardware-address*</code>	Specifies the hardware address of a DHCP client	DC
<code>host*</code>	Specifies the IP address and network mask to manually bind to a DHCP client	DC
<code>lease</code>	Sets the duration an IP address is assigned to a DHCP client	DC
<code>netbios-name-server</code>	Configures NetBIOS Windows Internet Naming Service (WINS) name servers available to Microsoft DHCP clients	DC
<code>netbios-node-type</code>	Configures NetBIOS node type for Microsoft DHCP clients	DC
<code>network</code>	Configures the subnet number and mask for a DHCP address pool	DC
<code>next-server</code>	Configures the next server in the boot process of a DHCP client	DC
<code>clear ip dhcp binding</code>	Deletes an automatic address binding from the DHCP server database	PE
<code>show ip dhcp binding</code>	Displays address bindings on the DHCP server	PE, NE
<code>show ip dhcp</code>	Displays DHCP address pools	PE

* These commands are used for manually binding an address to a client.

ip dhcp excluded-address This command specifies IP addresses that the DHCP server should not assign to DHCP clients. Use the **no** form to remove the excluded IP addresses.

Syntax

[no] ip dhcp excluded-address *low-address* [*high-address*]

low-address - An excluded IP address, or the first IP address in an excluded address range.

high-address - The last IP address in an excluded address range.

Default Setting

All IP pool addresses may be assigned.

Command Mode

Global Configuration

Example

```
Console(config)#ip dhcp excluded-address 10.1.0.19
Console(config)#
```

ip dhcp pool This command configures a DHCP address pool and enter DHCP Pool Configuration mode. Use the **no** form to remove the address pool.

Syntax

[no] ip dhcp pool *name*

name - A string or integer. (Range: 1-8 characters)

Default Setting

DHCP address pools are not configured.

Command Mode

Global Configuration

Usage Guidelines

- ◆ After executing this command, the switch changes to DHCP Pool Configuration mode, identified by the (config-dhcp)# prompt.
- ◆ From this mode, first configure address pools for the network interfaces (using the [network](#) command). You can also manually bind an address to a specific client (with the [host](#) command) if required. You can configure up to 8 network address pools, and up to 32 manually bound host address pools (i.e., listing one host address per pool). However, note that any address specified in a [host](#) command must fall within the range of a configured network address pool.

Example

```
Console(config)#ip dhcp pool R&D
Console(config-dhcp)#
```

Related Commands

[network \(746\)](#)

[host \(743\)](#)

service dhcp This command enables the DHCP server on this switch. Use the **no** form to disable the DHCP server.

Syntax

[no] service dhcp

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

If the DHCP server is running, you must restart it to implement any configuration changes.

Example

```
Console(config)#service dhcp
Console(config)#
```

bootfile This command specifies the name of the default boot image for a DHCP client. This file should be placed on the Trivial File Transfer Protocol (TFTP) server specified with the [next-server](#) command. Use the **no** form to delete the boot image name.

Syntax

bootfile *filename*

no bootfile

filename - Name of the file that is used as a default boot image.

Default Setting

None

Command Mode

DHCP Pool Configuration

Example

```
Console(config-dhcp)#bootfile wme.bat
Console(config-dhcp)#
```

Related Commands

[next-server \(747\)](#)

client-identifier This command specifies the client identifier of a DHCP client. Use the **no** form to remove the client identifier.

Syntax

client-identifier {**text** *text* | **hex** *hex*}

no client-identifier

text - A text string. (Range: 1-15 characters)

hex - The hexadecimal value.

Default Setting

None

Command Mode

DHCP Pool Configuration

Command Usage

- ◆ This command identifies a DHCP client to bind to an address specified in the [host](#) command. If both a client identifier and hardware address are configured for a host address, the client identifier takes precedence over the hardware address in the search procedure.
- ◆ BOOTP clients cannot transmit a client identifier. To bind an address to a BOOTP client, you must associate a hardware address with the host entry.

Example

```
Console(config-dhcp) #client-identifier text steve  
Console(config-dhcp) #
```

Related Commands

[host \(743\)](#)

default-router This command specifies default routers for a DHCP pool. Use the **no** form to remove the default routers.

Syntax

default-router *address1* [*address2*]

no default-router

address1 - Specifies the IP address of the primary router.

address2 - Specifies the IP address of an alternate router.

Default Setting

None

Command Mode

DHCP Pool Configuration

Usage Guidelines

The IP address of the router should be on the same subnet as the client. You can specify up to two routers. Routers are listed in order of preference (starting with *address1* as the most preferred router).

Example

```
Console(config-dhcp) #default-router 10.1.0.54 10.1.0.64  
Console(config-dhcp) #
```

dns-server This command specifies the Domain Name System (DNS) IP servers available to a DHCP client. Use the **no** form to remove the DNS server list.

Syntax

dns-server *address1* [*address2*]

no dns-server

address1 - Specifies the IP address of the primary DNS server.

address2 - Specifies the IP address of the alternate DNS server.

Default Setting

None

Command Mode

DHCP Pool Configuration

Usage Guidelines

- ◆ If DNS IP servers are not configured for a DHCP client, the client cannot correlate host names to IP addresses.
- ◆ Servers are listed in order of preference (starting with *address1* as the most preferred server).

Example

```
Console(config-dhcp)#dns-server 10.1.1.253 192.168.3.19
Console(config-dhcp)#
```

domain-name This command specifies the domain name for a DHCP client. Use the **no** form to remove the domain name.

Syntax

domain-name *domain*

no domain-name

domain - Specifies the domain name of the client.
(Range: 1-32 characters)

Default Setting

None

Command Mode

DHCP Pool Configuration

Example

```
Console(config-dhcp)#domain-name sample.com
Console(config-dhcp)#
```

hardware-address This command specifies the hardware address of a DHCP client. This command is valid for manual bindings only. Use the **no** form to remove the hardware address.

Syntax

hardware-address *hardware-address type*

no hardware-address

hardware-address - Specifies the MAC address of the client device.

type - Indicates the following protocol used on the client device:

- ethernet
- ieee802
- fddi

Default Setting

If no type is specified, the default protocol is Ethernet.

Command Mode

DHCP Pool Configuration

Command Usage

This command identifies a DHCP or BOOTP client to bind to an address specified in the [host](#) command. BOOTP clients cannot transmit a client identifier. To bind an address to a BOOTP client, you must associate a hardware address with the host entry.

Example

```
Console(config-dhcp)#hardware-address 00-e0-29-94-34-28 ethernet
Console(config-dhcp)#
```

Related Commands

[host \(743\)](#)

host Use this command to specify the IP address and network mask to manually bind to a DHCP client. Use the **no** form to remove the IP address for the client.

Syntax

host *address* [*mask*]

no host

address - Specifies the IP address of a client.

mask - Specifies the network mask of the client.

Default Setting

None

Command Mode

DHCP Pool Configuration

Usage Guidelines

- ◆ Host addresses must fall within the range specified for an existing network pool.
- ◆ When a client request is received, the switch first checks for a network address pool matching the gateway where the request originated (i.e., if the request was forwarded by a relay server). If there is no gateway in the client request (i.e., the request was not forwarded by a relay server), the switch searches for a network pool matching the interface through which the client request was received. It then searches for a manually configured host address that falls within the matching network pool.
- ◆ When searching for a manual binding, the switch compares the client identifier for DHCP clients, and then compares the hardware address for DHCP or BOOTP clients.
- ◆ If no manual binding has been specified for a host entry with the [client-identifier](#) or [hardware-address](#) commands, then the switch will assign an address from the matching network pool.
- ◆ If the mask is unspecified, DHCP examines its address pools. If no mask is found in the pool database, the Class A, B, or C natural mask is used (see [page 746](#)). This command is valid for manual bindings only.
- ◆ The **no host** command only clears the address from the DHCP server database. It does not cancel the IP address currently in use by the host.

Example

```
Console(config-dhcp)#host 10.1.0.21 255.255.255.0
Console(config-dhcp)#
```

Related Commands

[client-identifier \(739\)](#)

[hardware-address \(742\)](#)

lease This command configures the duration that an IP address is assigned to a DHCP client. Use the **no** form to restore the default value.

Syntax

lease {*days* [*hours*] [*minutes*] | **infinite**}

no lease

days - Specifies the duration of the lease in numbers of days. (Range: 0-364)

hours - Specifies the number of hours in the lease. A *days* value must be supplied before you can configure *hours*. (Range: 0-23)

minutes - Specifies the number of minutes in the lease. A *days* and *hours* value must be supplied before you can configure *minutes*. (Range: 0-59)

infinite - Specifies that the lease time is unlimited. This option is normally used for addresses manually bound to a BOOTP client via the **host** command.

Default Setting

One day

Command Modes

DHCP Pool Configuration

Example

The following example leases an address to clients using this pool for 7 days.

```
Console(config-dhcp)#lease 7
Console(config-dhcp)#
```

netbios-name-server This command configures NetBIOS Windows Internet Naming Service (WINS) name servers that are available to Microsoft DHCP clients. Use the **no** form to remove the NetBIOS name server list.

Syntax

netbios-name-server *address1* [*address2*]

no netbios-name-server

address1 - Specifies IP address of primary NetBIOS WINS name server.

address2 - Specifies IP address of alternate NetBIOS WINS name server.

Default Setting

None

Command Mode

DHCP Pool Configuration

Usage Guidelines

Servers are listed in order of preference (starting with *address1* as the most preferred server).

Example

```
Console(config-dhcp)#netbios-name-server 10.1.0.33 10.1.0.34
Console(config-dhcp)#
```

Related Commands

[netbios-node-type \(745\)](#)

netbios-node-type This command configures the NetBIOS node type for Microsoft DHCP clients. Use the **no** form to remove the NetBIOS node type.

Syntax

netbios-node-type *type*

no netbios-node-type

type - Specifies the NetBIOS node type:

broadcast

hybrid (recommended)

mixed

peer-to-peer

Default Setting

None

Command Mode

DHCP Pool Configuration

Example

```
Console(config-dhcp)#netbios-node-type hybrid
Console(config-dhcp)#
```

Related Commands

[netbios-name-server \(744\)](#)

network This command configures the subnet number and mask for a DHCP address pool. Use the **no** form to remove the subnet number and mask.

Syntax

network *network-number* [*mask*]

no network

network-number - The IP address of the DHCP address pool.

mask - The bit combination that identifies the network (or subnet) and the host portion of the DHCP address pool.

Command Mode

DHCP Pool Configuration

Usage Guidelines

- ◆ When a client request is received, the switch first checks for a network address pool matching the gateway where the request originated (i.e., if the request was forwarded by a relay server). If there is no gateway in the client request (i.e., the request was not forwarded by a relay server), the switch searches for a network pool matching the interface through which the client request was received. It then searches for a manually configured host address that falls within the matching network pool. If no manually configured host address is found, it assigns an address from the matching network address pool. However, if no matching address pool is found the request is ignored.
- ◆ This command is valid for DHCP network address pools only. If the mask is not specified, the class A, B, or C natural mask is used. Subnet addresses are interpreted as class A, B or C, based on the first field in the specified address. In other words, if a subnet address *nnn.xxx.xxx.xxx* is entered, the first field (*nnn*) determines the class:
 - 0 - 127 is class A, only uses the first field in the network address.
 - 128 - 191 is class B, uses the first two fields in the network address.
 - 192 - 223 is class C, uses the first three fields in the network address.
- ◆ The DHCP server assumes that all host addresses are available. You can exclude subsets of the address space by using the [ip dhcp excluded-address](#) command.

Example

```
Console(config-dhcp) #network 10.1.0.0 255.255.255.0
Console(config-dhcp) #
```

next-server This command configures the next server in the boot process of a DHCP client. Use the **no** form to remove the boot server list.

Syntax

[no] next-server *address*

address - Specifies the IP address of the next server in the boot process, which is typically a Trivial File Transfer Protocol (TFTP) server.

Default Setting

None

Command Mode

DHCP Pool Configuration

Example

```
Console(config-dhcp)#next-server 10.1.0.21
Console(config-dhcp)#
```

Related Commands

[bootfile \(739\)](#)

clear ip dhcp binding This command deletes an automatic address binding from the DHCP server database.

Syntax

clear ip dhcp binding {*address* | *}

address - The address of the binding to clear.

* - Clears all automatic bindings.

Default Setting

None

Command Mode

Privileged Exec

Usage Guidelines

- ◆ An *address* specifies the client's IP address. If an asterisk (*) is used as the address parameter, the DHCP server clears all automatic bindings.
- ◆ Use the **no host** command to delete a manual binding.
- ◆ This command is normally used after modifying the address pool, or after moving DHCP service to another device.

Example.

```
Console#clear ip dhcp binding *
Console#
```

Related Commands

[show ip dhcp binding \(748\)](#)

show ip dhcp binding This command displays address bindings on the DHCP server.

Syntax

show ip dhcp binding [*address*]

address - Specifies the IP address of the DHCP client for which bindings will be displayed.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show ip dhcp binding

      IP                MAC                Lease Time                Start
      (dd/hh/mm/ss)
-----
      192.1.3.21  00-00-e8-98-73-21                86400 Dec 25 08:01:57 2002
Console#
```

show ip dhcp This command displays DHCP address pools configured on the switch.

Command Mode

Privileged Exec

Example

```
Console#show ip dhcp

      Name    Type    IP Address                Mask                Active Pool
-----
      tps     Net    192.168.1.0                255.255.255.0        192.168.1.1 - 192.168.1.254

Total entry : 1
Console#
```

IP Interface Commands

An IP Version 4 and Version 6 address may be used for management access to the switch over the network. Both IPv4 or IPv6 addresses can be used simultaneously to access the switch. You can manually configure a specific IPv4 or IPv6 address or direct the switch to obtain an IPv4 address from a BOOTP or DHCP server when it is powered on. To ensure that this router resides at a known location in the network, a global IPv6 address can only be manually configured.

An IPv4 address for this switch is obtained via DHCP by default for VLAN 1. You may also need to establish an IPv4 or IPv6 default gateway between this device and management stations that exist on another network segment.

Table 160: IP Interface Commands

Command Group	Function
IPv4 Interface	Configures an IPv4 address for the switch
IPv6 Interface	Configures an IPv6 address for the switch
IPv6 to IPv4 Tunnels	Configures IPv6 over IPv4 tunnels

IPv4 Interface

An IPv4 address is assigned to this switch using DHCP by default. If this address is not suitable, you can manually configure a new address to manage the switch over your network or to connect the switch to existing IP subnets. You may also need to establish a default gateway between this device and management stations or other devices that exist on another network segment (if routing is not enabled).

This section includes commands for configuring IP interfaces, the Address Resolution Protocol (ARP) and Proxy ARP.

Table 161: IPv4 Interface Commands

Command Group	Function
Basic IPv4 Configuration	Configures the IP address for interfaces and the gateway router
ARP Configuration	Configures static, dynamic and proxy ARP service
UDP Helper Configuration	Forwards UDP broadcast packets to a specified server

Basic IPv4 Configuration This section describes commands used to configure IP addresses for VLAN interfaces on the switch.

Table 162: Basic IP Configuration Commands

Command	Function	Mode
<code>ip address</code>	Sets the IP address for the current interface	IC
<code>ip default-gateway</code>	Defines the default gateway through which this switch can reach other subnetworks	GC
<code>show ip interface</code>	Displays the IP settings for this device	PE
<code>show ip traffic</code>	Displays statistics for IP, ICMP, UDP, TCP and ARP protocols	PE
<code>tracert</code>	Shows the route packets take to the specified host	PE
<code>ping</code>	Sends ICMP echo request packets to another node on the network	NE, PE

ip address This command sets the IPv4 address for the currently selected VLAN interface. Use the **no** form to restore the default IP address.

Syntax

[no] ip address {ip-address netmask [secondary] | bootp | dhcp}

ip-address - IP address

netmask - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.

secondary - Specifies a secondary IP address.

bootp - Obtains IP address from BOOTP.

dhcp - Obtains IP address from DHCP.

Default Setting

DHCP

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ If this router is directly connected to end node devices (or connected to end nodes via shared media) that will be assigned to a specific subnet, then you must create a router interface for each VLAN that will support routing. The router interface consists of an IP address and subnet mask. This interface address defines both the network number to which the router interface is attached and the router's host number on that network. In other words, a router interface address defines the network and subnetwork numbers of the segment that is connected to that interface, and allows you to send IP packets to or from the router.

- ◆ Before any network interfaces are configured on the router, first create a VLAN for each unique user group, or for each network application and its associated users. Then assign the ports associated with each of these VLANs.
- ◆ An IP address must be assigned to this device to gain management access over the network or to connect the router to existing IP subnets. A specific IP address can be manually configured, or the router can be directed to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Anything other than this format will not be accepted by the configuration program.
- ◆ An interface can have only one primary IP address, but can have many secondary IP addresses. In other words, secondary addresses need to be specified if more than one IP subnet can be accessed through this interface. Note that a secondary address cannot be configured prior to setting the primary IP address, and the primary address cannot be removed if a secondary address is still present. Also, if any router/switch in a network segment uses a secondary address, all other routers/switches in that segment must also use a secondary address from the same network or subnet address space.
- ◆ If **bootp** or **dhcp** options are selected, the system will immediately start broadcasting service requests for all VLANs configured to obtain address assignments through BOOTP or DHCP. IP is enabled but will not function until a BOOTP or DHCP reply has been received. Requests are broadcast periodically by the router in an effort to learn its IP address. (BOOTP and DHCP values can include the IP address, default gateway, and subnet mask). If the DHCP/BOOTP server is slow to respond, you may need to use the [ip dhcp restart client](#) command to re-start broadcasting service requests, or reboot the router.



Note: Each VLAN group can be assigned its own IP interface address. Therefore, if routing is enabled, you can manage the router via any of these IP addresses.

Example

In the following example, the device is assigned an address in VLAN 1.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#
```

Related Commands

[ip dhcp restart client \(731\)](#)

[ip default-gateway \(752\)](#)

[ipv6 address \(766\)](#)

ip default-gateway This command specifies the default gateway for destinations not found in the local routing tables. Use the **no** form to remove a default gateway.

Syntax

ip default-gateway *gateway*

no ip default-gateway

gateway - IP address of the default gateway

Default Setting

No default gateway is established.

Command Mode

Global Configuration

Command Usage

- ◆ The default gateway can also be defined using the following command:
ip route 0.0.0.0/0 *gateway-address*.
- ◆ Static routes can also be defined using the **ip route** command to ensure that traffic to the designated address or subnet passes through a preferred gateway.
- ◆ A default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the router.

Example

The following example defines a default gateway for this device:

```
Console(config)#ip default-gateway 10.1.1.254
Console(config)#
```

Related Commands

[ip address \(750\)](#)

[ip route \(812\)](#)

[ipv6 default-gateway \(765\)](#)

show ip interface This command displays the settings of an IPv4 interface.

Command Mode

Privileged Exec

Example

```
Console#show ip interface
VLAN 1 is Administrative Up - Link Up
Address is 00-00-0C-00-00-FD
Index: 1001, MTU: 1500
Address Mode is DHCP
```



```
IP Address: 192.168.0.3 Mask: 255.255.255.0
Proxy ARP is disabled
Console#
```

Related Commands

[ip address \(750\)](#)

[show ipv6 interface \(773\)](#)

show ip traffic This command displays statistics for IP, ICMP, UDP, TCP and ARP protocols.

Command Mode

Privileged Exec

Example

```
Console#show ip traffic
IP Statistics:
IP received
    4877 total received
        header errors
        unknown protocols
        address errors
        discards
    4763 delivers
        reassembly request datagrams
        reassembly succeeded
        reassembly failed
IP sent
    forwards datagrams
    5927 requests
        discards
        no routes
        generated fragments
        fragment succeeded
        fragment failed
ICMP Statistics:
ICMP received
    input
    errors
    destination unreachable messages
    time exceeded messages
    parameter problem message
    echo request messages
    echo reply messages
    redirect messages
    timestamp request messages
    timestamp reply messages
    source quench messages
    address mask request messages
    address mask reply messages
ICMP sent
    output
    errors
    destination unreachable messages
    time exceeded messages
    parameter problem message
    echo request messages
    echo reply messages
    redirect messages
```

```
timestamp request messages
timestamp reply messages
source quench messages
address mask request messages
address mask reply messages

UDP Statistics:
    2 input
    no port errors
    other errors
    output

TCP Statistics:
    4698 input
    input errors
    5867 output

Console#
```

traceroute This command shows the route packets take to the specified destination.

Syntax

traceroute *host*

host - IP address or alias of the host.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- ◆ Use the **traceroute** command to determine the path taken to reach a specified destination.
- ◆ A trace terminates when the destination responds, when the maximum timeout (TTL) is exceeded, or the maximum number of hops is exceeded.
- ◆ The traceroute command first sends probe datagrams with the TTL value set at one. This causes the first router to discard the datagram and return an error message. The trace function then sends several probe messages at each subsequent TTL level and displays the round-trip time for each message. Not all devices respond correctly to probes by returning an "ICMP port unreachable" message. If the timer goes off before a response is returned, the trace function prints a series of asterisks and the "Request Timed Out" message. A long sequence of these messages, terminating only when the maximum timeout has been reached, may indicate this problem with the target device.

- ◆ If the target device does not respond or other errors are detected, the switch will indicate this by one of the following messages:
 - * - No Response
 - H - Host Unreachable
 - N - Network Unreachable
 - P - Protocol Unreachable
 - O -Other

Example

```

Console#traceroute 192.168.0.1
Press "ESC" to abort.
Traceroute to 192.168.1.99, 30 hops max, timeout is 3 seconds

Hop  Packet 1 Packet 2 Packet 3 IP Address
-----
  1      20 ms   <10 ms   <10 ms 192.168.1.99

Trace completed.
Console#

```

ping This command sends (IPv4) ICMP echo request packets to another node on the network.

Syntax

ping *host* [**count** *count*] [**size** *size*]

host - IP address or IP alias of the host.

count - Number of packets to send. (Range: 1-16)

size - Number of bytes in a packet. (Range: 32-512)

The actual packet size will be eight bytes larger than the size specified because the router adds header information.

Default Setting

count: 5

size: 32 bytes

Command Mode

Normal Exec, Privileged Exec

Command Usage

- ◆ Use the ping command to see if another site on the network can be reached.
- ◆ The following are some results of the **ping** command:
 - *Normal response* - The normal response occurs in one to ten seconds, depending on network traffic.

- *Destination does not respond* - If the host does not respond, a “timeout” appears in ten seconds.
 - *Destination unreachable* - The gateway for this destination indicates that the destination is unreachable.
 - *Network or host unreachable* - The gateway found no corresponding entry in the route table.
- ◆ When pinging a host name, be sure the DNS server has been enabled (see [page 722](#)) and host name-to-address translation enabled (see [page 722](#)). If necessary, local devices can also be specified in the DNS static host table (see [page 724](#)).

Example

```
Console#ping 10.1.0.9
Type ESC to abort.
PING to 10.1.0.9, by 5 32-byte payload ICMP packets, timeout is 5 seconds
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 0 ms
Ping statistics for 10.1.0.9:
 5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
  Minimum = 0 ms, Maximum = 10 ms, Average = 8 ms
Console#
```

Related Commands

[interface \(370\)](#)

ARP Configuration This section describes commands used to configure the Address Resolution Protocol (ARP) on the switch.

Table 163: Address Resolution Protocol Commands

Command	Function	Mode
arp	Adds a static entry in the ARP cache	GC
arp timeout	Sets the time a dynamic entry remains in the ARP cache	GC
ip proxy-arp	Enables proxy ARP service	IC
clear arp-cache	Deletes all dynamic entries from the ARP cache	PE
show arp	Displays entries in the ARP cache	NE, PE

arp This command adds a static entry in the Address Resolution Protocol (ARP) cache. Use the **no** form to remove an entry from the cache.

Syntax

arp *ip-address hardware-address*

no arp *ip-address*

ip-address - IP address to map to a specified hardware address.

hardware-address - Hardware address to map to a specified IP address. (The format for this address is xx-xx-xx-xx-xx-xx.)

Default Setting

No default entries

Command Mode

Global Configuration

Command Usage

- ◆ The ARP cache is used to map 32-bit IP addresses into 48-bit hardware (i.e., Media Access Control) addresses. This cache includes entries for hosts and other routers on local network interfaces defined on this router.
- ◆ The maximum number of static entries allowed in the ARP cache is 128.
- ◆ You may need to enter a static entry in the cache if there is no response to an ARP broadcast message. For example, some applications may not respond to ARP requests or the response arrives too late, causing network operations to time out.
- ◆ Static entries will not be aged out nor deleted when power is reset. A static entry can only be removed through the configuration interface.

Example

```
Console(config)#arp 10.1.0.19 01-02-03-04-05-06
Console(config)#
```

Related Commands

[clear arp-cache \(759\)](#)

[show arp \(759\)](#)

arp timeout This command sets the aging time for dynamic entries in the Address Resolution Protocol (ARP) cache. Use the **no** form to restore the default timeout.

Syntax

arp timeout *seconds*

no arp timeout

seconds - The time a dynamic entry remains in the ARP cache.
(Range: 300-86400; 86400 seconds is one day)

Default Setting

1200 seconds (20 minutes)

Command Mode

Global Configuration

Command Usage

- ◆ When a ARP entry expires, it is deleted from the cache and an ARP request packet is sent to re-establish the MAC address.
- ◆ The aging time determines how long dynamic entries remain in the cache. If the timeout is too short, the router may tie up resources by repeating ARP requests for addresses recently flushed from the table.

Example

This example sets the ARP cache timeout for 15 minutes (i.e., 900 seconds).

```
Console(config)#arp timeout 900
Console(config)#
```

ip proxy-arp This command enables proxy Address Resolution Protocol (ARP). Use the **no** form to disable proxy ARP.

Syntax

[no] ip proxy-arp

Default Setting

Disabled

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ Proxy ARP allows a non-routing device to determine the MAC address of a host on another subnet or network.

- ◆ End stations that require Proxy ARP must view the entire network as a single network. These nodes must therefore use a smaller subnet mask than that used by the router or other relevant network devices.
- ◆ Extensive use of Proxy ARP can degrade router performance because it may lead to increased ARP traffic and increased search time for larger ARP address tables.

Example

```
Console(config)#interface vlan 3
Console(config-if)#ip proxy-arp
Console(config-if)#
```

clear arp-cache This command deletes all dynamic entries from the Address Resolution Protocol (ARP) cache.

Command Mode

Privileged Exec

Example

This example clears all dynamic entries in the ARP cache.

```
Console#clear arp-cache
This operation will delete all the dynamic entries in ARP Cache.
Are you sure to continue this operation (y/n)?y
Console#
```

show arp This command displays entries in the Address Resolution Protocol (ARP) cache.

Command Mode

Normal Exec, Privileged Exec

Command Usage

- ◆ This command displays information about the ARP cache. The first line shows the cache timeout. It also shows each cache entry, including the IP address, MAC address, type (static, dynamic, other), and VLAN interface. Note that entry type "other" indicates local addresses for this router.
- ◆ Static entries are only displayed for VLANs that are up. In other words, static entries are only displayed when configured for the IP subnet of a existing VLAN, and that VLAN is linked up.

Example

This example displays all entries in the ARP cache.

```
Console#show arp
ARP Cache Timeout: 1200 (seconds)

IP Address      MAC Address      Type      Interface
-----
10.1.0.0        FF-FF-FF-FF-FF-FF other      VLAN1
10.1.0.254      00-00-AB-CD-00-00 other      VLAN1
10.1.0.255      FF-FF-FF-FF-FF-FF other      VLAN1
145.30.20.23    09-50-40-30-20-10 dynamic    VLAN3

Total entry : 5
Console#
```

UDP Helper Configuration

User Datagram Protocol (UDP) Helper allows host applications to forward UDP broadcast packets from this switch to another part of the network. This section describes the commands used to configure UDP Helper.

Table 164: UDP Helper Commands

Command	Function	Mode
ip forward-protocol udp	Specifies the UDP destination ports for which broadcast traffic will be forwarded	GC
ip helper	Enables UDP helper globally on the switch	GC
ip helper-address	Specifies the servers to which designated UDP protocol packets are forwarded	IC
show ip helper	Displays configuration settings for UDP helper	PE

[ip forward-protocol udp](#)

This command specifies the UDP destination ports for which broadcast traffic will be forwarded when the UDP helper is enabled. Use the **no** form to remove a UDP port from the forwarding list.

Syntax

[no] ip forward-protocol udp *destination-port*

destination-port - UDP application port for which UDP service requests are forwarded. (Range: 1-65535)

Default Setting

The following UDP ports are included in the forwarding list when UDP helper is enabled with the [ip helper](#) command and a remote server address is configured with the [ip helper-address](#) command:

BOOTP client port 67
BOOTP server port 68
Domain Name Service port 53

IEN-116 Name Service port 42
NetBIOS Datagram Server port 138
NetBIOS Name Server port 137
NTP port 37
TACACS service port 49
TFTP port 69

Command Mode

Global Configuration

Command Usage

Up to 100 UDP ports can be specified with this command for forwarding to one or more remote servers.

Example

This example enables forwarding for DHCPv6 UDP packets.

```
Console(config)#ip forward-protocol udp 547  
Console(config)#
```

ip helper This command enables UDP helper globally on the switch. Use the **no** form to disable this feature.

Syntax

[no] ip helper

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ Network hosts occasionally use UDP broadcasts to determine information such as address configuration, and domain name mapping. These broadcasts are confined to the local subnet, either as an all hosts broadcast (all ones broadcast - 255.255.255.255), or a directed subnet broadcast (such as 10.10.10.255). To reduce the number of application servers deployed in a multi-segment network, UDP helper can be used to forward broadcast packets for specified UDP application ports to remote servers located in another network segment.
- ◆ To configure UDP helper, it must be enabled globally with the **ip helper** command. The UDP destination ports for which broadcast traffic will be forwarded must be specified with the **ip forward-protocol udp** command. And

the remote servers which are configured to service UDP clients on another network segment specified with the [ip helper-address](#) command.

Example

This example enables UDP helper globally on the switch.

```
Console(config)#ip helper  
Console(config)#
```

ip helper-address This command specifies the application server or subnet (indicated by a directed broadcast address) to which designated UDP broadcast packets are forwarded. Use the **no** form to remove a UDP helper address.

Syntax

[no] ip helper-address *ip-address*

ip-address - Host address or directed broadcast address to which UDP broadcast packets are forwarded. (Range: 1-65535)

Default Setting

None

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ Up to 20 helper addresses can be specified with this command.
- ◆ To forward UDP packets with the UDP helper, the clients must be connected to the selected interface, and the interface configured with an IP address.
- ◆ The UDP packets to be forwarded must be specified by the [ip forward-protocol udp](#) command, and the packets meet the following criteria:
 - The MAC address of the received frame must be all-ones broadcast address (ffff.ffff.ffff).
 - The IP destination address must be one of the following:
 - all-ones broadcast (255.255.255.255)
 - subnet broadcast for the receiving interface
 - The IP time-to-live (TTL) value must be at least 2.
 - The IP protocol must be UDP (17).

- The UDP destination port must be TFTP, Domain Name System (DNS), Time, NetBIOS, BOOTP or DHCP packet, or a UDP port specified by the `ip forward-protocol udp` command.
- ◆ If a helper address is specified with this command, but no UDP ports have been specified with the `ip forward-protocol udp` command, broadcast traffic for several UDP protocol types will be forwarded by default as described under the `ip forward-protocol udp` command.

Example

This example indicates that designated UDP broadcast packets are to be forwarded to the directed broadcast address of 192.168.2.255.

```
Console(config)#interface vlan 1
Console(config-if)#ip helper-address 192.168.2.255
Console(config-if)#
```

show ip helper This command displays configuration settings for UDP helper.

Command Mode

Privileged Exec

Command Usage

This command displays all configuration settings for UDP helper, including its functional status, the UDP ports for which broadcast traffic will be forwarded, and the remote servers or subnets to which the traffic will be forwarded.

Example

```
Console#show ip helper
Helper mechanism is enabled
Forward port list(maximum count: 100)
  547
Total port number now is: 1
Helper address list(maximum count: 1024)
Interface VLAN 1:
  192.168.1.44
  192.168.2.255
Total helper number now is: 2

Console#
```

IPv6 Interface

This switch supports the following IPv6 interface commands.

Table 165: IPv6 Configuration Commands

Command	Function	Mode
<i>Interface Address Configuration and Utilities</i>		
<code>ipv6 default-gateway</code>	Sets an IPv6 default gateway for traffic with no known next hop	GC
<code>ipv6 address</code>	Configures an IPv6 global unicast address, and enables IPv6 on an interface	IC
<code>ipv6 address eui-64</code>	Configures an IPv6 global unicast address for an interface using an EUI-64 interface ID in the low order 64 bits, and enables IPv6 on the interface	IC
<code>ipv6 address link-local</code>	Configures an IPv6 link-local address for an interface and enables IPv6 on the interface	IC
<code>ipv6 enable</code>	Enables IPv6 on an interface that has not been configured with an explicit IPv6 address	IC
<code>ipv6 mtu</code>	Sets the size of the maximum transmission unit (MTU) for IPv6 packets sent on an interface	IC
<code>show ipv6 interface</code>	Displays the usability and configured settings for IPv6 interfaces	NE, PE
<code>show ipv6 mtu</code>	Displays maximum transmission unit (MTU) information for IPv6 interfaces	NE, PE
<code>show ipv6 traffic</code>	Displays statistics about IPv6 traffic	NE, PE
<code>clear ipv6 traffic</code>	Resets IPv6 traffic counters	PE
<code>ping6</code>	Sends IPv6 ICMP echo request packets to another node on the network	PE
<code>tracert6</code>	Shows the route packets take to the specified host	PE
<i>Neighbor Discovery</i>		
<code>ipv6 hop-limit</code>	Configures the maximum number of hops used in all IPv6 packets originated by this router	GC
<code>ipv6 nd dad attempts</code>	Configures the number of consecutive neighbor solicitation messages sent on an interface during duplicate address detection	IC
<code>ipv6 nd ns-interval</code>	Configures the interval between IPv6 neighbor solicitation retransmissions on an interface	IC
<code>ipv6 nd rguard</code>	Blocks incoming Router Advertisement and Router Redirect packets	IC
<code>ipv6 nd reachable-time</code>	Configures the amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred	IC
<code>ipv6 neighbor</code>	Configures a static entry in the IPv6 neighbor discovery cache	GC
<code>clear ipv6 neighbors</code>	Deletes all dynamic entries in the IPv6 neighbor discovery cache	PE

Table 165: IPv6 Configuration Commands (Continued)

Command	Function	Mode
<code>show ipv6 nd raguard</code>	Displays the configuration setting for RA Guard	PE
<code>show ipv6 neighbors</code>	Displays information in the IPv6 neighbor discovery cache	PE

Interface Address Configuration and Utilities

ipv6 default-gateway This command sets an IPv6 default gateway to use for destinations with no known next hop. Use the **no** form to remove a previously configured default gateway.

Syntax

ipv6 default-gateway *ipv6-address*

no ipv6 address

ipv6-address - The IPv6 address of the default next hop router to use for destinations with no known next hop.

Default Setting

No default gateway is defined

Command Mode

Global Configuration

Command Usage

- ◆ All IPv6 addresses must be according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
- ◆ The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address, include zone-id information indicating the VLAN identifier after the % delimiter. For example, FE80::7272%1 identifies VLAN 1 as the interface from which the ping is sent.
- ◆ An IPv6 default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the router.
- ◆ An IPv6 default gateway must be defined if a destination is located in a different IP segment and routing is disabled.

Example

The following example defines a default gateway for this device:

```
Console(config)#ipv6 default-gateway FE80::269:3EF9:FE19:6780%1
Console(config)#
```

Related Commands

[ip route \(812\)](#)
[show ip route \(814\)](#)
[ip default-gateway \(752\)](#)

ipv6 address This command configures an IPv6 global unicast address and enables IPv6 on an interface. Use the **no** form without any arguments to remove all IPv6 addresses from the interface, or use the **no** form with a specific IPv6 address to remove that address from the interface.

Syntax

[no] ipv6 address *ipv6-address*[/*prefix-length*]

ipv6-address - A full IPv6 address including the network prefix and host address bits.

prefix-length - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

Default Setting

No IPv6 addresses are defined

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ All IPv6 addresses must be according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
- ◆ To connect to a larger network with multiple subnets, you must configure a global unicast address. This address can be manually configured with this command.
- ◆ If a link-local address has not yet been assigned to this interface, this command will assign the specified static global unicast address and also dynamically generate a link-local unicast address for the interface. (The link-local address is made with an address prefix of FE80 and a host portion based the switch's MAC address in modified EUI-64 format.)
- ◆ If a duplicate address is detected, a warning message is sent to the console.

Example

This example specifies a full IPv6 address and prefix length.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address 2001:DB8:2222:7272::72/96
```

```

Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
    fe80::2e0:cff:fe02:fd%1/64
Global unicast address(es):
    2001:db8:2222:7272::72/96, subnet is 2001:db8:2222:7272::/96
Joined group address(es):
    ff02::2
    ff02::1:ff00:0
    ff02::1:ff00:72
    ff02::1:ff02:fd
    ff02::1:2
    ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 1.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds

Console#

```

Related Commands

[ipv6 address eui-64 \(767\)](#)

[show ipv6 interface \(773\)](#)

[ip address \(750\)](#)

ipv6 address eui-64 This command configures an IPv6 address for an interface using an EUI-64 interface ID in the low order 64 bits and enables IPv6 on the interface. Use the **no** form without any arguments to remove all manually configured IPv6 addresses from the interface. Use the **no** form with a specific address to remove it from the interface.

Syntax

ipv6 address *ipv6-prefix/prefix-length* eui-64

no ipv6 address [*ipv6-prefix/prefix-length* eui-64]

ipv6-prefix - The IPv6 network portion of the address assigned to the interface.

prefix-length - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

Default Setting

No IPv6 addresses are defined

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ The prefix must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
- ◆ If a link local address has not yet been assigned to this interface, this command will dynamically generate a global unicast address and a link-local address for this interface. (The link-local address is made with an address prefix of FE80 and a host portion based the switch’s MAC address in modified EUI-64 format.)
- ◆ Note that the value specified in the ipv6-prefix may include some of the high-order host bits if the specified prefix length is less than 64 bits. If the specified prefix length exceeds 64 bits, then the network portion of the address will take precedence over the interface identifier.
- ◆ If a duplicate address is detected, a warning message is sent to the console.
- ◆ IPv6 addresses are 16 bytes long, of which the bottom 8 bytes typically form a unique host identifier based on the device’s MAC address. The EUI-64 specification is designed for devices that use an extended 8-byte MAC address. For devices that still use a 6-byte MAC address (also known as EUI-48 format), it must be converted into EUI-64 format by inverting the universal/local bit in the address and inserting the hexadecimal number FFFE between the upper and lower three bytes of the MAC address.
- ◆ For example, if a device had an EUI-48 address of 28-9F-18-1C-82-35, the global/local bit must first be inverted to meet EUI-64 requirements (i.e., 1 for globally defined addresses and 0 for locally defined addresses), changing 28 to 2A. Then the two bytes FFFE are inserted between the OUI (i.e., company id) and the rest of the address, resulting in a modified EUI-64 interface identifier of 2A-9F-18-FF-FE-1C-82-35.
- ◆ This host addressing method allows the same interface identifier to be used on multiple IP interfaces of a single device, as long as those interfaces are attached to different subnets.

Example

This example uses the network prefix of 2001:0DB8:0:1::/64, and specifies that the EUI-64 interface identifier be used in the lower 64 bits of the address.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address 2001:0DB8:0:1::/64 eui-64
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enable.
Link-local address:
  2001:db8:0:1:2e0:cff:fe02:fd/64, subnet is 2001:db8:0:1::/64[EUI]
  2001:db8:2222:7272::72/96, subnet is 2001:db8:2222:7272::/96
Joined group address(es):
ff02::2
```



```
ff02::1:ff00:0
ff02::1:ff00:72
ff02::1:ff02:fd
ff02::1:2
ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 1.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds
```

Console#

Related Commands

[show ipv6 interface \(773\)](#)

ipv6 address link-local This command configures an IPv6 link-local address for an interface and enables IPv6 on the interface. Use the **no** form without any arguments to remove all manually configured IPv6 addresses from the interface. Use the **no** form with a specific address to remove it from the interface.

Syntax

ipv6 address *ipv6-address* link-local

no ipv6 address [*ipv6-address* link-local]

ipv6-address - The IPv6 address assigned to the interface.

Default Setting

No IPv6 addresses are defined

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ The specified address must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. And the address prefix must be in the range of FE80~FEBF.
- ◆ The address specified with this command replaces a link-local address that was automatically generated for the interface.
- ◆ You can configure multiple IPv6 global unicast addresses per interface, but only one link-local address per interface.
- ◆ If a duplicate address is detected, a warning message is sent to the console.

Example

This example assigns a link-local address of FE80::269:3EF9:FE19:6779 to VLAN 1. Note that a prefix in the range of FE80~FEBF is required for link-local addresses, and the first 16-bit group in the host address is padded with a zero in the form 0269.

```
Console(config)#interface tunnel 1
Console(config-if)#ipv6 address FE80::269:3EF9:FE19:6779 link-local
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
    fe80::269:3ef9:fe19:6779%1/64
Global unicast address(es):
    2001:db8:0:1:2e0:cff:fe02:fd/64, subnet is 2001:db8:0:1::/64[EUI]
    2001:db8:2222:7272::72/96, subnet is 2001:db8:2222:7272::/96
Joined group address(es):
    ff02::2
    ff02::1:ff19:6779
    ff02::1:ff00:0
    ff02::1:ff00:72
    ff02::1:ff02:fd
    ff02::1:2
    ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 1.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds
Console#
```

Related Commands

[ipv6 enable \(770\)](#)

[show ipv6 interface \(773\)](#)

ipv6 enable This command enables IPv6 on an interface that has not been configured with an explicit IPv6 address. Use the **no** form to disable IPv6 on an interface that has not been configured with an explicit IPv6 address.

Syntax

[no] ipv6 enable

Default Setting

IPv6 is disabled

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ This command enables IPv6 on the current VLAN interface and automatically generates a link-local unicast address. The address prefix uses FE80, and the

host portion of the address is generated by converting the switch's MAC address to modified EUI-64 format (see [page 767](#)). This address type makes the switch accessible over IPv6 for all devices attached to the same local subnet.

- ◆ If a duplicate address is detected on the local segment, this interface will be disabled and a warning message displayed on the console.
- ◆ The **no ipv6 enable** command does not disable IPv6 for an interface that has been explicitly configured with an IPv6 address.

Example

In this example, IPv6 is enabled on VLAN 1, and the link-local address FE80::2E0:CFF:FE00:FD/64 is automatically generated by the switch.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 enable
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
    fe80::269:3ef9:fe19:6779%1/64
Global unicast address(es):
    2001:db8:0:1:2e0:cff:fe02:fd/64, subnet is 2001:db8:0:1::/64[EUI]
    2001:db8:2222:7272::72/96, subnet is 2001:db8:2222:7272::/96
Joined group address(es):
    ff02::2
    ff02::1:ff19:6779
    ff02::1:ff00:0
    ff02::1:ff00:72
    ff02::1:ff02:fd
    ff02::1:2
    ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 1.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds

Console#
```

Related Commands

[ipv6 address link-local \(769\)](#)
[show ipv6 interface \(773\)](#)

ipv6 mtu This command sets the size of the maximum transmission unit (MTU) for IPv6 packets sent on an interface. Use the **no** form to restore the default setting.

Syntax

ipv6 mtu *size*

no ipv6 mtu

size - Specifies the MTU size. (Range: 1280-65535 bytes)

Default Setting

1500 bytes

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ If a non-default value is configured, an MTU option is included in the router advertisements sent from this device.
- ◆ The maximum value set by this command cannot exceed the MTU of the physical interface, which is currently fixed at 1500 bytes.
- ◆ IPv6 routers do not fragment IPv6 packets forwarded from other routers. However, traffic originating from an end-station connected to an IPv6 router may be fragmented.
- ◆ All devices on the same physical medium must use the same MTU in order to operate correctly.
- ◆ IPv6 must be enabled on an interface before the MTU can be set.

Example

The following example sets the MTU for VLAN 1 to 1280 bytes:

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 mtu 1280
Console(config-if)#
```

Related Commands

[show ipv6 mtu \(775\)](#)

[jumbo frame \(122\)](#)

show ipv6 interface This command displays the usability and configured settings for IPv6 interfaces.

Syntax

show ipv6 interface [**brief** [**vlan** *vlan-id* [*ipv6-prefix/prefix-length*]]]

brief - Displays a brief summary of IPv6 operational status and the addresses configured for each interface.

vlan-id - VLAN ID (Range: 1-4094)

ipv6-prefix - The IPv6 network portion of the address assigned to the interface. The prefix must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

prefix-length - A decimal value indicating how many of the contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

Command Mode

Normal Exec, Privileged Exec

Example

This example displays all the IPv6 addresses configured for the switch.

```
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
    fe80::269:3ef9:fe19:6779%1/64
Global unicast address(es):
    2001:db8:0:1:2e0:cff:fe02:fd/64, subnet is 2001:db8:0:1::/64[EUI]
    2001:db8:2222:7272::72/96, subnet is 2001:db8:2222:7272::/96
Joined group address(es):
    ff02::2
    ff02::1:ff19:6779
    ff02::1:ff00:0
    ff02::1:ff00:72
    ff02::1:ff02:fd
    ff02::1:2
    ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 1.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds

Console#
```

Table 166: show ipv6 interface - display description

Field	Description
VLAN	A VLAN is marked "up" if the switch can send and receive packets on this interface, "down" if a line signal is not present, or "administratively down" if the interface has been disabled by the administrator.
IPv6	IPv6 is marked "enable" if the switch can send and receive IP traffic on this interface, "disable" if the switch cannot send and receive IP traffic on this interface, or "stalled" if a duplicate link-local address is detected on the interface.
Link-local address	Shows the link-local address assigned to this interface
Global unicast address(es)	Shows the global unicast address(es) assigned to this interface
Joined group address(es)	<p>In addition to the unicast addresses assigned to an interface, a node is required to join the all-nodes multicast addresses FF01::1 and FF02::1 for all IPv6 nodes within scope 1 (interface-local) and scope 2 (link-local), respectively.</p> <p>FF01::1/16 is the transient interface-local multicast address for all attached IPv6 nodes, and FF02::1/16 is the link-local multicast address for all attached IPv6 nodes. The interface-local multicast address is only used for loopback transmission of multicast traffic. Link-local multicast addresses cover the same types as used by link-local unicast addresses, including all nodes (FF02::1), all routers (FF02::2), and solicited nodes (FF02::1:FFXX:XXXX) as described below.</p> <p>A node is also required to compute and join the associated solicited-node multicast addresses for every unicast and anycast address it is assigned. IPv6 addresses that differ only in the high-order bits, e.g. due to multiple high-order prefixes associated with different aggregations, will map to the same solicited-node address, thereby reducing the number of multicast addresses a node must join. In this example, FF02::1:FF90:0/104 is the solicited-node multicast address which is formed by taking the low-order 24 bits of the address and appending those bits to the prefix.</p>
MTU	Maximum transmission unit for this interface.
ND DAD	Indicates whether (neighbor discovery) duplicate address detection is enabled.
number of DAD attempts	The number of consecutive neighbor solicitation messages sent on the interface during duplicate address detection.
ND retransmit interval	The interval between IPv6 neighbor solicitation retransmissions sent on an interface during duplicate address detection.
ND advertised retransmit interval	The retransmit interval is included in all router advertisements sent out of an interface so that nodes on the same link use the same time value.
ND reachable time	The amount of time a remote IPv6 node is considered reachable after a reachability confirmation event has occurred
ND advertised reachable time	The reachable time is included in all router advertisements sent out of an interface so that nodes on the same link use the same time value.
ND advertised router lifetime	Tells the neighbor receiving this message how long this router should be used as a default router.

This example displays a brief summary of IPv6 addresses configured on the switch.

```

Console#show ipv6 interface brief
Interface      VLAN      IPv6      IPv6 Address
-----
VLAN 1         Up        Up        2001:db8:0:1:2e0:cff:fe02:fd/64
VLAN 1         Up        Up        2001:db8:2222:7272::72/96
VLAN 1         Up        Up        fe80::269:3ef9:fe19:6779/64

```

```
Craft      Up      Down      Unassigned
Console#
```

Related Commands

[show ip interface \(752\)](#)

show ipv6 mtu This command displays the maximum transmission unit (MTU) cache for destinations that have returned an ICMP packet-too-big message along with an acceptable MTU to this switch.

Command Mode

Normal Exec, Privileged Exec

Example

The following example shows the MTU cache for this device:

```
Console#show ipv6 mtu
MTU      Since      Destination Address
1400     00:04:21    5000:1::3
1280     00:04:50    FE80::203:A0FF:FED6:141D
Console#
```

Table 167: show ipv6 mtu - display description*

Field	Description
MTU	Adjusted MTU contained in the ICMP packet-too-big message returned from this destination, and now used for all traffic sent along this path.
Since	Time since an ICMP packet-too-big message was received from this destination.
Destination Address	Address which sent an ICMP packet-too-big message.

* No information is displayed if an IPv6 address has not been assigned to the switch.

show ipv6 traffic This command displays statistics about IPv6 traffic passing through this switch.

Command Mode

Normal Exec, Privileged Exec

Example

The following example shows statistics for all IPv6 unicast and multicast traffic, as well as ICMP, UDP and TCP statistics:

```
Console#show ipv6 traffic
IPv6 Statistics:
IPv6 received                total received
                             header errors
```

```

too big errors
no routes
address errors
unknown protocols
truncated packets
discards
delivers
reassembly request datagrams
reassembly succeeded
reassembly failed

IPv6 sent
15 forwards datagrams
requests
discards
no routes
generated fragments
fragment succeeded
fragment failed

ICMPv6 Statistics:
ICMPv6 received
input
errors
destination unreachable messages
packet too big messages
time exceeded messages
parameter problem message
echo request messages
echo reply messages
router solicit messages
router advertisement messages
neighbor solicit messages
neighbor advertisement messages
redirect messages
group membership query messages
group membership response messages
group membership reduction messages
multicast listener discovery version 2 reports

ICMPv6 sent
4 output
destination unreachable messages
packet too big messages
time exceeded messages
parameter problem message
echo request messages
echo reply messages
3 router solicit messages
router advertisement messages
1 neighbor solicit messages
neighbor advertisement messages
redirect messages
group membership query messages
group membership response messages
group membership reduction messages
multicast listener discovery version 2 reports

UDP Statistics:
input
no port errors
other errors
output

Console#
```


Table 168: show ipv6 traffic - display description

Field	Description
<i>IPv6 Statistics</i>	
<i>IPv6 recived</i>	
total received	The total number of input datagrams received by the interface, including those received in error.
header errors	The number of input datagrams discarded due to errors in their IPv6 headers, including version number mismatch, other format errors, hop count exceeded, IPv6 options, etc.
too big errors	The number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface.
no routes	The number of input datagrams discarded because no route could be found to transmit them to their destination.
address errors	The number of input datagrams discarded because the IPv6 address in their IPv6 header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., ::0) and unsupported addresses (e.g., addresses with unallocated prefixes). For entities which are not IPv6 routers and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
unknown protocols	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the datagrams.
truncated packets	The number of input datagrams discarded because datagram frame didn't carry enough data.
discards	The number of input IPv6 datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
delivers	The total number of datagrams successfully delivered to IPv6 user-protocols (including ICMP). This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the datagrams.
reassembly request datagrams	The number of IPv6 fragments received which needed to be reassembled at this interface. Note that this counter is incremented at the interface to which these fragments were addressed which might not be necessarily the input interface for some of the fragments.
reassembly succeeded	The number of IPv6 datagrams successfully reassembled. Note that this counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the fragments.
reassembly failed	The number of failures detected by the IPv6 re-assembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IPv6 fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received. This counter is incremented at the interface to which these fragments were addressed which might not be necessarily the input interface for some of the fragments.

Table 168: show ipv6 traffic - display description (Continued)

Field	Description
<i>IPv6 sent</i>	
forwards datagrams	The number of output datagrams which this entity received and forwarded to their final destinations. In entities which do not act as IPv6 routers, this counter will include only those packets which were Source-Routed via this entity, and the Source-Route processing was successful. Note that for a successfully forwarded datagram the counter of the outgoing interface is incremented.
requests	The total number of IPv6 datagrams which local IPv6 user-protocols (including ICMP) supplied to IPv6 in requests for transmission. Note that this counter does not include any datagrams counted in <code>ipv6IfStatsOutForwDatagrams</code> .
discards	The number of output IPv6 datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in <code>ipv6IfStatsOutForwDatagrams</code> if any such packets met this (discretionary) discard criterion.
no routes	The number of input datagrams discarded because no route could be found to transmit them to their destination.
generated fragments	The number of output datagram fragments that have been generated as a result of fragmentation at this output interface.
fragment succeeded	The number of IPv6 datagrams that have been successfully fragmented at this output interface.
fragment failed	The number of IPv6 datagrams that have been discarded because they needed to be fragmented at this output interface but could not be.
<i>ICMPv6 Statistics</i>	
<i>ICMPv6 received</i>	
input	The total number of ICMP messages received by the interface which includes all those counted by <code>ipv6IfIcmpInErrors</code> . Note that this interface is the interface to which the ICMP messages were addressed which may not be necessarily the input interface for the messages.
errors	The number of ICMP messages which the interface received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).
destination unreachable messages	The number of ICMP Destination Unreachable messages received by the interface.
packet too big messages	The number of ICMP Packet Too Big messages received by the interface.
time exceeded messages	The number of ICMP Time Exceeded messages received by the interface.
parameter problem message	The number of ICMP Parameter Problem messages received by the interface.
echo request messages	The number of ICMP Echo (request) messages received by the interface.
echo reply messages	The number of ICMP Echo Reply messages received by the interface.
router solicit messages	The number of ICMP Router Solicit messages received by the interface.
router advertisement messages	The number of ICMP Router Advertisement messages received by the interface.

Table 168: show ipv6 traffic - display description (Continued)

Field	Description
neighbor solicit messages	The number of ICMP Neighbor Solicit messages received by the interface.
neighbor advertisement messages	The number of ICMP Neighbor Advertisement messages received by the interface.
redirect messages	The number of Redirect messages received by the interface.
group membership query messages	The number of ICMPv6 Group Membership Query messages received by the interface.
group membership response messages	The number of ICMPv6 Group Membership Response messages received by the interface.
group membership reduction messages	The number of ICMPv6 Group Membership Reduction messages received by the interface.
multicast listener discovery version 2 reports	The number of MLDv2 reports received by the interface.
<i>ICMPv6 sent</i>	
output	The total number of ICMP messages which this interface attempted to send. Note that this counter includes all those counted by icmpOutErrors.
destination unreachable messages	The number of ICMP Destination Unreachable messages sent by the interface.
packet too big messages	The number of ICMP Packet Too Big messages sent by the interface.
time exceeded messages	The number of ICMP Time Exceeded messages sent by the interface.
parameter problem message	The number of ICMP Parameter Problem messages sent by the interface.
echo request messages	The number of ICMP Echo (request) messages sent by the interface.
echo reply messages	The number of ICMP Echo Reply messages sent by the interface.
router solicit messages	The number of ICMP Router Solicitation messages sent by the interface.
router advertisement messages	The number of ICMP Router Advertisement messages sent by the interface.
neighbor solicit messages	The number of ICMP Neighbor Solicit messages sent by the interface.
neighbor advertisement messages	The number of ICMP Router Advertisement messages sent by the interface.
redirect messages	The number of Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
group membership query messages	The number of ICMPv6 Group Membership Query messages sent by the interface.
group membership response messages	The number of ICMPv6 Group Membership Response messages sent.
group membership reduction messages	The number of ICMPv6 Group Membership Reduction messages sent.
multicast listener discovery version 2 reports	The number of MLDv2 reports sent by the interface.
<i>UDP Statistics</i>	
input	The total number of UDP datagrams delivered to UDP users.

Table 168: show ipv6 traffic - display description (Continued)

Field	Description
no port errors	The total number of received UDP datagrams for which there was no application at the destination port.
other errors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
output	The total number of UDP datagrams sent from this entity.

clear ipv6 traffic This command resets IPv6 traffic counters.

Command Mode

Privileged Exec

Command Usage

This command resets all of the counters displayed by the **show ipv6 traffic** command.

Example

```
Console#clear ipv6 traffic
Console#
```

ping6 This command sends (IPv6) ICMP echo request packets to another node on the network.

Syntax

ping6 {*ipv6-address* | *host-name*} [**count** *count*] [**size** *size*]

ipv6-address - The IPv6 address of a neighbor device. You can specify either a link-local or global unicast address formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

host-name - A host name string which can be resolved into an IPv6 address through a domain name server.

count - Number of packets to send. (Range: 1-16)

size - Number of bytes in a packet. (Range: 48-18024 bytes)

The actual packet size will be eight bytes larger than the size specified because the router adds header information.

Default Setting

count: 5

size: 100 bytes

Command Mode

Privileged Exec

Command Usage

- ◆ Use the **ping6** command to see if another site on the network can be reached, or to evaluate delays over the path.
- ◆ The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address, include zone-id information indicating the VLAN identifier after the % delimiter. For example, FE80::7272%1 identifies VLAN 1 as the interface from which the ping is sent.
- ◆ When pinging a host name, be sure the DNS server has been enabled (see [page 722](#)). If necessary, local devices can also be specified in the DNS static host table (see [page 724](#)).
- ◆ When using ping6 with a host name, the router first attempts to resolve the alias into an IPv6 address before trying to resolve it into an IPv4 address.

Example

```

Console#ping6 FE80::2E0:CFF:FE00:FC%1/64
Type ESC to abort.
PING to FE80::2E0:CFF:FE00:FC%1/64, by 5 32-byte payload ICMP packets,
  timeout is 3 seconds
response time: 20 ms      [FE80::2E0:CFF:FE00:FC] seq_no: 1
response time: 0 ms      [FE80::2E0:CFF:FE00:FC] seq_no: 2
response time: 0 ms      [FE80::2E0:CFF:FE00:FC] seq_no: 3
response time: 0 ms      [FE80::2E0:CFF:FE00:FC] seq_no: 4
response time: 0 ms      [FE80::2E0:CFF:FE00:FC] seq_no: 5
Ping statistics for FE80::2E0:CFF:FE00:FC%1/64:
  5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
  Minimum = 0 ms, Maximum = 20 ms, Average = 4 ms
Console#

```

traceroute6 This command shows the route packets take to the specified destination.

Syntax

traceroute {*ipv6-address* | *host-name*} [**max-failures** *max-failures*]

ipv6-address - The IPv6 address of a neighbor device. You can specify either a link-local or global unicast address formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

host-name - A host name string which can be resolved into an IPv6 address through a domain name server.

max-failures - The maximum number of failures before which the trace route is terminated. (Range: 1-255; Default: 5)

Default Setting

Maximum failures: 5

Command Mode

Privileged Exec

Command Usage

- ◆ Use the **tracert** command to determine the path taken to reach a specified destination.
- ◆ The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address, include zone-id information indicating the VLAN identifier after the % delimiter. For example, FE80::7272%1 identifies VLAN 1 as the interface from which the ping is sent.
- ◆ A trace terminates when the destination responds, when the maximum timeout (TTL) is exceeded, or the maximum number of hops is exceeded.
- ◆ The tracert command first sends probe datagrams with the TTL value set at one. This causes the first router to discard the datagram and return an error message. The trace function then sends several probe messages at each subsequent TTL level and displays the round-trip time for each message. Not all devices respond correctly to probes by returning an "ICMP port unreachable" message. If the timer goes off before a response is returned, the trace function prints a series of asterisks and the "Request Timed Out" message. A long sequence of these messages, terminating only when the maximum timeout has been reached, may indicate this problem with the target device.

Example

```
Console#tracert FE80::2E0:CFF:FE9C:CA10%1/64
Press "ESC" to abort.

Tracert to FE80::2E0:CFF:FE9C:CA10%1/64, 30 hops max, timeout is 3
seconds, 5 max failure(s) before termination.

Hop  Packet 1 Packet 2 Packet 3 IPv6 Address
-----
 1    <10 ms   <10 ms   <10 ms FE80::2E0:CFF:FE9C:CA10%1/64

Trace completed.
Console#
```

Neighbor Discovery

ipv6 hop-limit This command configures the maximum number of hops used in all IPv6 packets originated by this router. Use the **no** form to restore the default setting.

Syntax

ipv6 hop-limit *hops*

no ipv6 hop-limit

hops - The maximum number of hops in all IPv6 packets. (Range: 1-255)

Default Setting

1

Command Mode

Global Configuration

Example

The following sets the hop limit to 64:

```
Console(config)#ipv6 hop-limit 64
Console(config)#
```

ipv6 nd dad attempts This command configures the number of consecutive neighbor solicitation messages sent on an interface during duplicate address detection. Use the **no** form to restore the default setting.

Syntax

ipv6 nd dad attempts *count*

no ipv6 nd dad attempts

count - The number of neighbor solicitation messages sent to determine whether or not a duplicate address exists on this interface. (Range: 0-600)

Default Setting

1

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ Configuring a value of 0 disables duplicate address detection.
- ◆ Duplicate address detection determines if a new unicast IPv6 address already exists on the network before it is assigned to an interface.

- ◆ Duplicate address detection is stopped on any interface that has been suspended (see the [vlan](#) command). While an interface is suspended, all unicast IPv6 addresses assigned to that interface are placed in a “pending” state. Duplicate address detection is automatically restarted when the interface is administratively re-activated.
- ◆ An interface that is re-activated restarts duplicate address detection for all unicast IPv6 addresses on the interface. While duplicate address detection is performed on the interface’s link-local address, the other IPv6 addresses remain in a “tentative” state. If no duplicate link-local address is found, duplicate address detection is started for the remaining IPv6 addresses.
- ◆ If a duplicate address is detected, it is set to “duplicate” state, and a warning message is sent to the console. If a duplicate link-local address is detected, IPv6 processes are disabled on the interface. If a duplicate global unicast address is detected, it is not used. All configuration commands associated with a duplicate address remain configured while the address is in “duplicate” state.
- ◆ If the link-local address for an interface is changed, duplicate address detection is performed on the new link-local address, but not for any of the IPv6 global unicast addresses already associated with the interface.

Example

The following configures five neighbor solicitation attempts for addresses configured on VLAN 1. The [show ipv6 interface](#) command indicates that the duplicate address detection process is still on-going.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 nd dad attempts 5
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
    fe80::269:3ef9:fe19:6779%1/64
Global unicast address(es):
    2001:db8:0:1:2e0:cff:fe02:fd/64, subnet is 2001:db8:0:1::/64[EUI]
    2001:db8:2222:7272::72/96, subnet is 2001:db8:2222:7272::/96
Joined group address(es):
    ff02::2
    ff02::1:ff19:6779
    ff02::1:ff00:0
    ff02::1:ff00:72
    ff02::1:ff02:fd
    ff02::1:2
    ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 5.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds

Console#
```


Related Commands

[ipv6 nd ns-interval \(785\)](#)

[show ipv6 neighbors \(790\)](#)

ipv6 nd ns-interval This command configures the interval between transmitting IPv6 neighbor solicitation messages on an interface. Use the **no** form to restore the default value.

Syntax

ipv6 nd ns-interval *milliseconds*

no ipv6 nd ns-interval

milliseconds - The interval between transmitting IPv6 neighbor solicitation messages. (Range: 1000-3600000)

Default Setting

1000 milliseconds is used for neighbor discovery operations

0 milliseconds is advertised in router advertisements

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ When a non-default value is configured, the specified interval is used both for router advertisements and by the router itself.
- ◆ This command specifies the interval between transmitting neighbor solicitation messages when resolving an address, or when probing the reachability of a neighbor. Therefore, avoid using very short intervals for normal IPv6 operations.
- ◆ Setting the neighbor solicitation interval to 0 means that the configured time is unspecified by this router.

Example

The following sets the interval between sending neighbor solicitation messages to 30000 milliseconds:

```
Console(config)#interface vlan 1
Console(config)#pv6 nd ns-interval 30000
Console(config)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
    fe80::269:3ef9:fe19:6779%1/64
Global unicast address(es):
    2001:db8:0:1:2e0:cff:fe02:fd/64, subnet is 2001:db8:0:1::/64[EUI]
    2001:db8:2222:7272::/96, subnet is 2001:db8:2222:7272::/96
Joined group address(es):
    ff02::2
```

```
ff02::1:ff19:6779
ff02::1:ff00:0
ff02::1:ff00:72
ff02::1:ff02:fd
ff02::1:2
ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 5.
ND retransmit interval is 30000 milliseconds
ND advertised retransmit interval is 30000 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds
```

Console#

Related Commands

[show running-config \(114\)](#)

ipv6 nd raguard This command blocks incoming Router Advertisement and Router Redirect packets. Use the no form to disable this feature.

Syntax

[no] ipv6 nd raguard

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ IPv6 Router Advertisements (RA) convey information that enables nodes to auto-configure on the network. This information may include the default router address taken from the observed source address of the RA message, as well as on-link prefix information. However, unintended misconfigurations, or possibly malicious attacks on the network, may lead to bogus RAs being sent, which in turn can cause operational problems for hosts on the network.
- ◆ This command can be used to block RAs and Router Redirect (RR) messages on the specified interface. Determine which interfaces are connected to known routers, and enable RA Guard on all other untrusted interfaces.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#pv6 nd raguard
Console(config-if)#
```

ipv6 nd reachable-time This command configures the amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred. Use the **no** form to restore the default setting.

Syntax

ipv6 nd reachable-time *milliseconds*

no ipv6 nd reachable-time

milliseconds - The time that a node can be considered reachable after receiving confirmation of reachability. (Range: 0-3600000)

Default Setting

30000 milliseconds is used for neighbor discovery operations
0 milliseconds is advertised in router advertisements

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ The time limit configured by this command allows the router to detect unavailable neighbors.
- ◆ This time limit is included in all router advertisements sent out through an interface, ensuring that nodes on the same link use the same time value.
- ◆ Setting the time limit to 0 means that the configured time is unspecified by this router.

Example

The following sets the reachable time for a remote node to 1000 milliseconds:

```
Console(config)#interface vlan 1
Console(config)#ipv6 nd reachable-time 1000
Console(config)#
```

ipv6 neighbor This command configures a static entry in the IPv6 neighbor discovery cache. Use the **no** form to remove a static entry from the cache.

Syntax

ipv6 neighbor *ipv6-address* **vlan** *vlan-id* *hardware-address*

no ipv6 mtu

ipv6-address - The IPv6 address of a neighbor device that can be reached through one of the network interfaces configured on this switch. You can specify either a link-local or global unicast address formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

vlan-id - VLAN ID (Range: 1-4094)

hardware-address - The 48-bit MAC layer address for the neighbor device. This address must be formatted as six hexadecimal pairs separated by hyphens.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ Address Resolution Protocol (ARP) has been replaced in IPv6 with the Neighbor Discovery Protocol (NDP). The **ipv6 neighbor** command is similar to the [mac-address-table static](#) command ([page 444](#)) that is implemented using ARP.
- ◆ Static entries can only be configured on an IPv6-enabled interface.
- ◆ The switch does not determine whether a static entry is reachable before placing it in the IPv6 neighbor discovery cache.
- ◆ If the specified entry was dynamically learned through the IPv6 neighbor discovery process, and already exists in the neighbor discovery cache, it is converted to a static entry. Static entries in the IPv6 neighbor discovery cache are not modified if subsequently detected by the neighbor discovery process.
- ◆ Disabling IPv6 on an interface with the [no ipv6 enable](#) command (see [page 770](#)) deletes all dynamically learned entries in the IPv6 neighbor discovery cache for that interface, but does not delete static entries.

Example

The following maps a static entry for global unicast address to a MAC address:

```
Console(config)#ipv6 neighbor 2009:DB9:2229::81 vlan 1 30-65-14-01-11-86
Console(config)#end
Console#show ipv6 neighbors
State: I1 - Incomplete, I2 - Invalid, R - Reachable, S - Stale, D - Delay,
       P1 - Probe, P2 - Permanent, U - Unknown
IPv6 Address      Age      Link-layer Addr   State      VLAN
2009:DB9:2229::80  956      12-34-11-11-43-21 R           1
2009:DB9:2229::81  Permanent 30-65-14-01-11-86 R           1
FE80::1034:11FF:FE11:4321 961      12-34-11-11-43-21 R           1
Console#
```

Related Commands

[show ipv6 neighbors \(790\)](#)

[mac-address-table static \(444\)](#)

clear ipv6 neighbors This command deletes all dynamic entries in the IPv6 neighbor discovery cache.

Command Mode

Privileged Exec

Example

The following deletes all dynamic entries in the IPv6 neighbor cache:

```
Console#clear ipv6 neighbors
Console#
```

show ipv6 nd raguard This command displays the configuration setting for RA Guard.

Syntax

show ipv6 nd raguard [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Command Mode

Privileged Exec

Example

```
Console#show ipv6 nd raguard interface ethernet 1/1
Interface RA Guard
-----
Eth 1/ 1   Yes
Console#
```

show ipv6 neighbors This command displays information in the IPv6 neighbor discovery cache.

Syntax

show ipv6 neighbors [**vlan** *vlan-id* | *ipv6-address*]

vlan-id - VLAN ID (Range: 1-4094)

ipv6-address - The IPv6 address of a neighbor device. You can specify either a link-local or global unicast address formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

Default Setting

All IPv6 neighbor discovery cache entries are displayed.

Command Mode

Privileged Exec

Example

The following shows all known IPv6 neighbors for this switch:

```
Console#show ipv6 neighbors
State: I1 - Incomplete, I2 - Invalid, R - Reachable, S - Stale, D - Delay,
       P1 - Probe, P2 - Permanent, U - Unknown
IPv6 Address          Age      Link-layer Addr   State VLAN
FE80::2E0:CFF:FE9C:CA10 4        00-E0-0C-9C-CA-10    R      1
Console#
```

Table 169: show ipv6 neighbors - display description

Field	Description
IPv6 Address	IPv6 address of neighbor
Age	The time since the address was verified as reachable (in seconds). A static entry is indicated by the value "Permanent."
Link-layer Addr	Physical layer MAC address.

Table 169: show ipv6 neighbors - display description (Continued)

Field	Description
State	<p>The following states are used for dynamic entries:</p> <p>I1 (Incomplete) - Address resolution is being carried out on the entry. A neighbor solicitation message has been sent to the multicast address of the target, but it has not yet returned a neighbor advertisement message.</p> <p>I2 (Invalid) - An invalidated mapping. Setting the state to invalid dis-associates the interface identified with this entry from the indicated mapping (RFC 4293).</p> <p>R (Reachable) - Positive confirmation was received within the last ReachableTime interval that the forward path to the neighbor was functioning. While in REACH state, the device takes no special action when sending packets.</p> <p>S (Stale) - More than the ReachableTime interval has elapsed since the last positive confirmation was received that the forward path was functioning. While in STALE state, the device takes no action until a packet is sent.</p> <p>D (Delay) - More than the ReachableTime interval has elapsed since the last positive confirmation was received that the forward path was functioning. A packet was sent within the last DELAY_FIRST_PROBE_TIME interval. If no reachability confirmation is received within this interval after entering the DELAY state, the switch will send a neighbor solicitation message and change the state to PROBE.</p> <p>P1 (Probe) - A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer interval until confirmation of reachability is received.</p> <p>U (Unknown) - Unknown state.</p> <p>The following states are used for static entries:</p> <p>I1 (Incomplete)-The interface for this entry is down.</p> <p>R (Reachable) - The interface for this entry is up. Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache.</p> <p>P2 (Permanent) - Indicates a static entry.</p>
VLAN	VLAN interface from which the address was reached.

Related Commands[show mac-address-table \(445\)](#)

IPv6 to IPv4 Tunnels

This switch supports connection between isolated IPv6 nodes over IPv4 networks using manually configured tunnels (RFC 2893), as well as the connection of isolated IPv6 domains over IPv4 clouds without explicit tunnel configuration (RFC 3056).

Table 170: IPv6 to IPv4 Tunnelling Commands

Command	Function	Mode
interface tunnel	Configures a tunnel interface and enters tunnel configuration mode	GC
ipv6 address	Configures an IPv6 global unicast address, and enables IPv6 on an interface	IC (tunnel)
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 on the interface	IC (tunnel)

Table 170: IPv6 to IPv4 Tunnelling Commands (Continued)

Command	Function	Mode
<code>ipv6 address eui-64</code>	Configures an IPv6 global unicast address for an interface using an EUI-64 interface ID in the low order 64 bits, and enables IPv6 on the interface	IC (tunnel)
<code>tunnel destination*</code>	Configures the IPv4 address of a tunnel destination	IC (tunnel)
<code>tunnel mode ipv6ip</code>	Configures the tunnel mode to manual configuration or 6-to-4 automatic tunneling	IC (tunnel)
<code>tunnel source vlan</code>	Sets the VLAN to which a tunnel source is assigned	IC (tunnel)
<code>tunnel ttl</code>	Configures the TTL value in the IPv4 header of a packet used for tunneling IPv6 traffic	IC (tunnel)
<code>show ipv6 tunnel</code>	Displays the status and configuration settings for all IPv6 over IPv4 tunnels	PE

* The tunnel destination only applies to manually configured tunneling (RFC 2893).

Command Usage

To create a manually configured or automatically configured tunnel, follow these steps:

1. Configure a VLAN with the `vlan` command.
2. Assign the ports which will use this VLAN for local services, and those which will form the entry point for the IPv6 over IPv4 tunnel (using the `switchport allowed vlan` command).
3. Assign an IPv4 address to the VLAN to serve as the source (or local end point) of the tunnel using the `ip address` command.
4. Create an IPv6 over IPv4 tunnel using the `interface tunnel` command.
5. Set the tunnel mode to "configured" for host-to-router or router-to-router connections, or "6to4" for router-to-host or host-to-host connections using the `tunnel mode ipv6ip` command.
6. For "configured" tunnel mode, specify the IPv4 address of the far end of the tunnel using the `tunnel destination` command.
7. Bind the tunnel to a VLAN with the `tunnel source vlan` command.
8. Assign an IPv6 global unicast address to the tunnel using the `ipv6 address` command.
9. Then check your configuration settings using the `show ipv6 tunnel` command, and the interface status of the tunnel using the `show ipv6 interface` or `show ipv6 interface brief` command.

interface tunnel This command configures an IPv6 to IPv4 tunnel interface and enters tunnel configuration mode. Use the **no** form with a tunnel number to remove a tunnel, or without a tunnel number to remove all tunnels.

Syntax

interface tunnel *tunnel-number*

no interface tunnel [*tunnel-number*]

tunnel-number - Tunnel interface identifier. (Range: 1-16)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ Although this command is labeled with the name “tunnel,” it allows configuration of either a manually configured IPv6 over IPv4 transport network based on RFC 2893, or of an automatic method of transporting IPv6 traffic over IPv4 clouds without explicit tunnels using RFC 3056.
- ◆ Configured IPv6 over IPv4 tunneling uses point-to-point tunnels by encapsulating IPv6 packets within IPv4 headers to carry them over IPv4 routing infrastructures.
- ◆ Transporting IPv6 over IPv4 clouds (based on RFC 3056) defines a method for assigning a unique IPv6 address prefix to any site that currently has at least one globally unique IPv4 address, and specifies an encapsulation mechanism for transmitting IPv6 packets using such a prefix over the global IPv4 network.

Example

```
Console(config)#interface tunnel 1
Console(config-if)#
```

tunnel destination This command sets the IPv4 address of a tunnel destination (or far end-point of a tunnel). Use the **no** form to remove the assigned IPv4 address.

Syntax

tunnel destination *ip-address*

no tunnel destination

ip-address - IPv4 address of the device at the far end of the tunnel.

Default Setting

None

Command Mode

Interface Configuration (IPv6/v4 Tunnel)

Command Usage

- ◆ This command is only applicable to the “configured” tunnel mode (see the [tunnel mode ipv6ip](#) command).
- ◆ When an IPv6 packet is transmitted over a tunnel, the tunnel end-point address configured by this command is used as the destination address for the encapsulating IPv4 header.
- ◆ The determination of which packets to tunnel is based on information in the routing table, which directs packets based on their destination address using the prefix mask and match technique.
- ◆ IPv6/IPv4 hosts that are connected to data links with no IPv6 routers may use a configured tunnel to reach an IPv6 router. This tunnel allows the host to communicate with the rest of the IPv6 Internet (i.e., nodes with IPv6-native addresses). If the IPv4 address of an IPv6/IPv4 router bordering the IPv6 backbone is known, this can be used as the tunnel end-point address. This tunnel can be configured into the routing table as an IPv6 “default route.” That is, all IPv6 destination addresses will match the route and could potentially traverse the tunnel. Since the “mask length” of such a default route is zero, it will be used only if there are no other routes with a longer mask that match the destination. Note that the default configured tunnel can also be used in conjunction with 6to4 automatic tunneling.
- ◆ The tunnel end-point address of a default tunnel could be the IPv4 address of one IPv6/IPv4 router at the border of the IPv6 backbone. Alternatively, the tunnel end point could be an IPv4 “anycast address.” Using this approach, multiple IPv6/IPv4 routers at the border advertise IPv4 reachability to the same IPv4 address. All of these routers accept packets to this address as their own, and will decapsulate IPv6 packets tunneled to this address. When an IPv6/IPv4 node sends an encapsulated packet to this address, it will be delivered to only one of the border routers, usually the closest one.
- ◆ Care must be taken when using a default tunnel to prevent different IPv4 fragments from arriving at different routers for reassembly. This can be prevented by either avoiding fragmentation of the encapsulated packets (by ensuring an IPv4 MTU of at least 1300 bytes is used) or by preventing frequent changes to IPv4 routing.
- ◆ Packets delivered to transport protocols on the decapsulating node should not be subject to ingress filtering. For bidirectionally configured tunnels this is done by verifying that the source address is the IPv4 address of the other end of the tunnel. For unidirectionally configured tunnels, the decapsulating node must be configured with a list of source IPv4 address prefixes that are acceptable. Such a list must default to not having any entries, i.e. the node has to be explicitly configured to forward decapsulated packets received over unidirectionally configured tunnels.

Example

```
Console(config)#interface tunnel 2
Console(config-if)#tunnel destination 192.168.1.5
Console(config-if)#
```

tunnel mode ipv6ip This command sets the tunnel mode to manual configuration or 6-to-4 automatic tunneling. Use the **no** form to restore the default setting.

Syntax

tunnel mode ipv6ip {configured | 6to4}

no tunnel mode ipv6ip

configured - Configured IPv6 over IPv4 tunneling using point-to-point tunnels by encapsulating IPv6 packets within IPv4 headers to carry them over IPv4 routing infrastructures (based on RFC 2893).

6to4 - Transports IPv6 over IPv4 clouds by assigning a unique IPv6 address prefix to any site that currently has at least one globally unique IPv4 address, and specifying an encapsulation mechanism for transmitting IPv6 packets using such a prefix over the global IPv4 network. (This method is based on RFC 3056.)

Default Setting

configured

Command Mode

Interface Configuration (IPv6/v4 Tunnel)

Command Usage

- ◆ Configured tunneling of IPv6 over IPv4 based on RFC 2893 uses point-to-point tunnels made by encapsulating IPv6 packets within IPv4 headers to carry them over IPv4 routing infrastructures. These tunnels can be either unidirectional or bidirectional. Bidirectionally configured tunnels behave as virtual point-to-point links. When using configured tunnels, the IPv4 tunnel end-point address must be manually configured on the encapsulating node with the **tunnel destination** command.

The 6to4 mechanism is typically implemented almost entirely in routers bordering between IPv4 and IPv6 domains.

The tunnel end-point address of a 6to4 tunnel is dynamically determined by the tunnel source (local end-point node) via the IPv6 6to4 address of the packet sent from IPv6 6to4 hosts. The 6to4 end-point address is constructed using "2002:Public IPv4 Address::/48" as the IPv6 address prefix. This prefix can be used exactly like any other valid IPv6 prefix, e.g., for "Neighbor Discovery for IP Version 6 (IPv6)" defined in RFC 2461.

- ◆ IPv6/IPv4 hosts and routers can tunnel IPv6 datagrams over regions of IPv4 routing topology by encapsulating them within IPv4 packets. Tunneling can be used in a variety of ways, including the following:
 - Router-to-Router: IPv6/IPv4 routers interconnected by an IPv4 infrastructure can tunnel IPv6 packets between themselves. In this case, the tunnel spans one segment of the end-to-end path that the IPv6 packet takes.
 - Host-to-Router: IPv6/IPv4 hosts can tunnel IPv6 packets to an intermediate IPv6/IPv4 router that is reachable via an IPv4 infrastructure. This type of tunnel spans the first segment of the packet's end-to-end path.
 - Host-to-Host: IPv6/IPv4 hosts that are interconnected by an IPv4 infrastructure can tunnel IPv6 packets between themselves. In this case, the tunnel spans the entire end-to-end path that the packet takes; and a host can be either a 6to4 node or native IPv6 host.
 - Router-to-Host: IPv6/IPv4 routers can tunnel IPv6 packets to their final destination IPv6/IPv4 host. This tunnel spans only the last segment of the end-to-end path.

Tunneling techniques are classified according to the mechanism by which the encapsulating node determines the address of the node at the end of the tunnel. In the first two tunneling methods listed above – router-to-router and host-to-router – the IPv6 packet is being tunneled to a router. The end point of this type of tunnel is an intermediate router which must decapsulate the IPv6 packet and forward it on to its final destination. When tunneling to a router, the end point of the tunnel is different from the destination of the packet being tunneled. So the addresses in the IPv6 packet being tunneled can not provide the IPv4 address of the tunnel end point. Instead, the tunnel end-point address must be determined from information configured on the encapsulating node. In other words, “configured tunneling” must be used to explicitly identify the end point.

In the last two tunneling methods – host-to-host and router-to-host – the IPv6 packet is tunneled all the way to its final destination. In this case, the destination address of both the IPv6 packet and the encapsulating IPv4 header identify the same node. This fact can be exploited by encoding information in the IPv6 destination address that will allow the encapsulating node to determine the tunnel end point IPv4 address automatically. “6to4 automatic tunneling” employs this technique, using a special IPv6 address format with an embedded IPv4 address to allow tunneling nodes to automatically derive the tunnel end-point IPv4 address. This eliminates the need to explicitly configure the tunnel end-point address.

- ◆ The two tunneling techniques – configured and automatic – differ primarily in how they determine the tunnel end-point address. Most of the underlying mechanisms are the same:
 - The entry node of the tunnel (the encapsulating node) creates an encapsulating IPv4 header and transmits the encapsulated packet.

- The exit node of the tunnel (the decapsulating node) receives the encapsulated packet, reassembles the packet if needed, removes the IPv4 header, updates the IPv6 header, and processes the received IPv6 packet.

Example

```
Console(config)#interface tunnel 2
Console(config-if)#tunnel mode ipv6ip configured
Console(config-if)#
```

tunnel source vlan This command sets the VLAN to which a tunnel source (or local end-point of a tunnel) is assigned. Use the **no** form to detach the tunnel from the assigned VLAN.

Syntax

tunnel source vlan *vlan-id*

no tunnel source vlan

vlan-id - VLAN ID (Range: 1-4094)

Default Setting

None

Command Mode

Interface Configuration (IPv6/v4 Tunnel)

Command Usage

The VLAN assigned to a tunnel must be a L3 VLAN with an IPv4 address. Otherwise, an error message will be displayed on the console.

Example

```
Console(config)#interface tunnel 2
Console(config-if)#tunnel source vlan 2
Console(config-if)#
```

tunnel ttl This command configures the TTL (Time to Live) value stored in the IPv4 header of a packet used for tunneling IPv6 traffic. Use the **no** form to restore the default value.

Syntax

tunnel ttl *ttl-value*

no tunnel ttl

ttl-value - The TTL value of the IPv4 encapsulating packet. (Range: 0-255, where zero means that the TTL value is taken from the Hop Limit set in the IP header of the encapsulated IPv6 packet)

Default Setting

0

Command Mode

Interface Configuration (IPv6/v4 Tunnel)

Command Usage

The command sets the hop limit for the IPv4 encapsulating packet. However, note that IPv6 over IPv4 tunnels are modeled as a “single-hop.” That is, the IPv6 hop limit is decremented by only one when an IPv6 packet traverses the tunnel. The single-hop model serves to hide the existence of a tunnel. The tunnel is opaque to users of the network, and is not detectable by network diagnostic tools such as traceroute.

Example

```
Console(config)#interface tunnel 2
Console(config-if)#tunnel ttl 5
Console(config-if)#
```

show ipv6 tunnel This command displays the status and configuration settings for all IPv6 over IPv4 tunnels.

Command Mode

Privileged Exec

Example

```
Console#show ipv6 tunnel

Tunnel:1
  Tunnel Current State           : Up
  Tunnel Source Address          : [VLAN1]192.168.0.3
  Tunnel Destination Address     : 192.168.0.2
  Time to Live                   : 255
  Tunnel Mode (Configured / 6-to-4) : Configured

Console#
```

The following example shows the interface status of the configured tunnels.

```
Console#show ipv6 interface
VLAN 1 is up
IPv6 is stale.
Link-local address:
(None)
Global unicast address(es):
(None)
Joined group address(es):
FF02::1:2
FF02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 2.
```

```
ND retransmit interval is 1000 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
```

```
Tunnel 1 is up
IPv6 is stale.
Link-local address:
  FE80::C0A8:3/64
Global unicast address(es):
  2002:DB9:2222:7272::72/48, subnet is 2002:DB9:2222::/48
Joined group address(es):
  FF02::1
IPv6 link MTU is 0 bytes
ND DAD is enabled, number of DAD attempts: 1.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds
```

```
Console#show ipv6 interface brief
```

Interface	VLAN	IPv6	IPv6 Address
VLAN 1	Up	Down	Unassigned
TUNNEL 1	Up	Down	2002:DB9:2222:7272::72/48
TUNNEL 1	Up	Down	FE80::C0A8:3

```
Console#
```


VRRP Commands

Virtual Router Redundancy Protocol (VRRP) use a virtual IP address to support a primary router and multiple backup routers. The backup routers can be configured to take over the workload if the master router fails, or can also be configured to share the traffic load. The primary goal of router redundancy is to allow a host device which has been configured with a fixed gateway to maintain network connectivity in case the primary gateway goes down.

To configure VRRP, select an interface on each router in the group that will participate in the protocol as the master router or a backup router. To select a specific device as the master router, set the address of this interface as the virtual router address for the group. Now set the same virtual address and a priority on the backup routers, and configure an authentication string. You can also enable the preempt feature which allows a router to take over as the master router when it comes on line if it has a higher priority than the currently active master router.

Table 171: VRRP Commands

Command	Function	Mode
<code>vrrp authentication</code>	Configures a key used to authenticate VRRP packets received from other routers	IC
<code>vrrp ip</code>	Enables VRRP and sets the IP address of the virtual router	IC
<code>vrrp preempt</code>	Configures the router to take over as master virtual router for a VRRP group if it has a higher priority than the current master virtual router	IC
<code>vrrp priority</code>	Sets the priority of this router in the VRRP group	IC
<code>vrrp timers advertise</code>	Sets the interval between successive advertisements by the master virtual router	IC
<code>clear vrrp interface counters</code>	Clears VRRP interface statistics	PE
<code>clear vrrp router counters</code>	Clears VRRP router statistics	PE
<code>show vrrp</code>	Displays VRRP status information	PE
<code>show vrrp interface</code>	Displays VRRP status information for the specified interface	PE
<code>show vrrp interface counters</code>	Displays VRRP statistics for the specified interface	PE
<code>show vrrp router counters</code>	Displays VRRP statistics	PE

vrrp authentication This command specifies the key used to authenticate VRRP packets received from other routers. Use the **no** form to prevent authentication.

Syntax

vrrp group authentication key

no vrrp group authentication

group - Identifies the virtual router group. (Range: 1-255)

key - Authentication string. (Range: 1-8 alphanumeric characters)

Default Setting

No key is defined.

Command Mode

Interface (VLAN)

Command Usage

- ◆ All routers in the same VRRP group must be configured with the same authentication key.
- ◆ When a VRRP packet is received from another router in the group, its authentication key is compared to the string configured on this router. If the keys match, the message is accepted. Otherwise, the packet is discarded.
- ◆ Plain text authentication does not provide any real security. It is supported only to prevent a misconfigured router from participating in VRRP.

Example

```
Console(config-if)#vrrp 1 authentication bluebird
Console(config-if)#
```

vrrp ip This command enables the Virtual Router Redundancy Protocol (VRRP) on an interface and specifies the IP address of the virtual router. Use the **no** form to disable VRRP on an interface and remove the IP address from the virtual router.

Syntax

[no] vrrp group ip ip-address

group - Identifies the virtual router group. (Range: 1-255)

ip-address - The IP address of the virtual router. This is the IP address that end-hosts set as their default gateway.

Default Setting

No virtual router groups are configured.

Command Mode

Interface (VLAN)

Command Usage

- ◆ The interfaces of all routers participating in a virtual router group must be within the same IP subnet.
- ◆ If the IP address assigned to the virtual router with this command is already configured as the primary address on this interface, this router is considered the Owner, and will assume the role of the Master virtual router in the group.
- ◆ This interface is used for two purposes - to send/receive advertisement messages and to forward on behalf of the virtual router when operating as the Master VRRP router.
- ◆ VRRP is enabled as soon as this command is entered. If you need to customize any of the other parameters for VRRP such as authentication, priority, or advertisement interval, then first configure these parameters before enabling VRRP.

Example

This example creates VRRP group 1 using the primary interface for VLAN 1 as the VRRP group Owner.

```

Console(config)#interface vlan 1
Console(config-if)#vrrp 1 ip 192.168.1.6
Console(config-if)#

```

vrrp preempt This command configures the router to take over as the master virtual router for a VRRP group if it has a higher priority than the current acting master router. Use the **no** form to disable preemption.

Syntax

vrrp group preempt [**delay** *seconds*]

no vrrp group preempt

group - Identifies the VRRP group. (Range: 1-255)

seconds - The time to wait before issuing a claim to become the master.
(Range: 0-120 seconds)

Default Setting

Preempt: Enabled

Delay: 0 seconds

Command Mode

Interface (VLAN)

Command Usage

- ◆ If preempt is enabled, and this backup router has a priority higher than the current acting master, it will take over as the new master. However, note that if the original master (i.e., the owner of the VRRP IP address) comes back on line, it will always resume control as the master.
- ◆ The delay can give additional time to receive an advertisement message from the current master before taking control. If the router attempting to become the master has just come on line, this delay also gives it time to gather information for its routing table before actually preempting the currently active router.

Example

```
Console(config-if)#vrrp 1 preempt delay 10
Console(config-if)#
```

Related Commands

[vrrp priority \(804\)](#)

vrrp priority This command sets the priority of this router in a VRRP group. Use the **no** form to restore the default setting.

Syntax

vrrp group priority level

no vrrp group priority

group - Identifies the VRRP group. (Range: 1-255)

level - Priority of this router in the VRRP group. (Range: 1-254)

Default Setting

Master: 255

Backup: 100

Command Mode

Interface (VLAN)

Command Usage

- ◆ A router that has a physical interface with the same IP address as that used for the virtual router (that is, the owner of the VRRP IP address) will become the master virtual router. The backup router with the highest priority will become the master router if the current master fails. When the original master router recovers, it will take over as the active master router again.
- ◆ If two or more routers are configured with the same VRRP priority, the router with the highest IP address is elected as the new master router if the current master fails.

- ◆ If the backup preempt function is enabled with the `vrrp preempt` command, and a backup router with a priority higher than the current acting master comes on line, this backup router will take over as the new acting master. However, note that if the original master (i.e., the owner of the VRRP IP address) comes back on line, it will always resume control as the master.
- ◆ If the virtual IP address for the VRRP group is the same as that of the configured device, the priority will automatically be set to 255 prior to using this command.

Example

```
Console(config-if)#vrrp 1 priority 1
Console(config-if)#
```

Related Commands

`vrrp preempt (803)`

vrrp timers advertise This command sets the interval at which the master virtual router sends advertisements communicating its state as the master. Use the **no** form to restore the default interval.

Syntax

vrrp group timers advertise interval

no vrrp group timers advertise

group - Identifies the VRRP group. (Range: 1-255)

interval - Advertisement interval for the master virtual router.
(Range: 1-255 seconds)

Default Setting

1 second

Command Mode

Interface (VLAN)

Command Usage

- ◆ VRRP advertisements from the current master virtual router include information about its priority and current state as the master.
- ◆ VRRP advertisements are sent to the multicast address 224.0.0.18. Using a multicast address reduces the amount of traffic that has to be processed by network devices that are not part of the designated VRRP group.
- ◆ If the master router stops sending advertisements, backup routers will bid to become the master router based on priority. The dead interval before

attempting to take over as the master is three times the hello interval plus half a second

Example

```
Console(config-if)#vrrp 1 timers advertise 5
Console(config-if)#
```

clear vrrp interface counters This command clears VRRP system statistics for the specified group and interface.

clear vrrp group interface interface counters

group - Identifies a VRRP group. (Range: 1-255)

interface - Identifier of configured VLAN interface. (Range: 1-4094)

Defaults

None

Command Mode

Privileged Exec

Example

```
Console#clear vrrp 1 interface 1 counters
Console#
```

clear vrrp router counters This command clears VRRP system statistics.

Command Mode

Privileged Exec

Example

```
Console#clear vrrp router counters
Console#
```

show vrrp This command displays status information for VRRP.

Syntax

show vrrp [**brief** | *group*]

brief - Displays summary information for all VRRP groups on this router.

group - Identifies a VRRP group. (Range: 1-255)

Defaults

None

Command Mode

Privileged Exec

Command Usage

- ◆ Use this command without any keywords to display the full listing of status information for all VRRP groups configured on this router.
- ◆ Use this command with the **brief** keyword to display a summary of status information for all VRRP groups configured on this router.
- ◆ Specify a group number to display status information for a specific group

Example

This example displays the full listing of status information for all groups.

```

Console#show vrrp
VLAN 1 - Group 1,
State                               Master
Virtual IP Address                  192.168.1.6
Virtual MAC Address                 00-00-5E-00-01-01
Advertisement Interval               5 sec
Preemption                         Enabled
Min Delay                           10 sec
Priority                             255
Authentication                      SimpleText
Authentication Key                  bluebird
Master Router                       192.168.1.6
Master Priority                      255
Master Advertisement Interval       5 sec
Master Down Interval                15
Console#

```

Table 172: show vrrp - display description

Field	Description
State	VRRP role of this interface (master or backup)
Virtual IP address	Virtual address that identifies this VRRP group
Virtual MAC address	Virtual MAC address derived from the owner of the virtual IP address
Advertisement interval	Interval at which the master virtual router advertises its role as the master
Preemption	Shows whether or not a higher priority router can preempt the current acting master
Min delay	Delay before a router with a higher priority can preempt the current acting master
Priority	Priority of this router
Authentication	Authentication mode used to verify VRRP packets
Authentication key	Key used to authenticate VRRP packets received from other routers

Table 172: show vrrp - display description (Continued)

Field	Description
Master Router	IP address of the router currently acting as the VRRP group master
Master priority	The priority of the router currently acting as the VRRP group master
Master Advertisement interval	The advertisement interval configured on the VRRP master.
Master down interval	The down interval configured on the VRRP master (This interval is used by all the routers in the group regardless of their local settings)

This example displays the brief listing of status information for all groups.

```

Console#show vrrp brief
Interface  Grp    State   Virtual Addr   Interval  Preempt  Priority
-----
VLAN 1    1    Master   192.168.0.3    1    E        255
Console#

```

Table 173: show vrrp brief - display description

Field	Description
Interface	VLAN interface
Grp	VRRP group
State	VRRP role of this interface (master or backup)
Virtual Addr	Virtual address that identifies this VRRP group
Interval	Interval at which the master virtual router advertises its role as the master
Preempt	Shows whether or not a higher priority router can preempt the current acting master
Priority	Priority of this router

show vrrp interface This command displays status information for the specified VRRP interface.

Syntax

show vrrp interface vlan *vlan-id* [**brief**]

vlan-id - Identifier of configured VLAN interface. (Range: 1-4094)

brief - Displays summary information for all VRRP groups on this router.

Defaults

None

Command Mode

Privileged Exec

Example

This example displays the full listing of status information for VLAN 1.

```

Console#show vrrp interface vlan 1
Vlan 1 - Group 1,
State                               Master
Virtual IP Address                  192.168.1.6
Virtual MAC Address                  00-00-5E-00-01-01
Advertisement Interval               5 sec
Preemption                          Enabled
Min Delay                           10 sec
Priority                             1
Authentication                      SimpleText
Authentication Key                  bluebird
Master Router                       192.168.1.6
Master Priority                      1
Master Advertisement Interval       5 sec
Master Down Interval                15
Console#

```

* Refer to the [show vrrp](#) command for a description of the display items.

show vrrp interface counters This command displays counters for VRRP protocol events and errors that have occurred for the specified group and interface.

show vrrp group interface vlan interface counters

group - Identifies a VRRP group. (Range: 1-255)

interface - Identifier of configured VLAN interface. (Range: 1-4094)

Defaults

None

Command Mode

Privileged Exec

Example

```

Console#show vrrp 1 interface vlan 1 counters
Total Number of Times Transitioned to MASTER                : 6
Total Number of Received Advertisements Packets             : 0
Total Number of Received Error Advertisement Interval Packets : 0
Total Number of Received Authentication Failures Packets    : 0
Total Number of Received Error IP TTL VRRP Packets          : 0
Total Number of Received Priority 0 VRRP Packets             : 0
Total Number of Sent Priority 0 VRRP Packets                 : 5
Total Number of Received Invalid Type VRRP Packets          : 0
Total Number of Received Error Address List VRRP Packets    : 0
Total Number of Received Invalid Authentication Type VRRP Packets : 0
Total Number of Received Mismatch Authentication Type VRRP Packets : 0
Total Number of Received Error Packet Length VRRP Packets   : 0
Console#

```

show vrrp router counters This command displays counters for errors found in VRRP protocol packets.

Command Mode

Privileged Exec

Example

Note that unknown errors indicate VRRP packets received with an unknown or unsupported version number.

```
Console#show vrrp router counters
Total Number of VRRP Packets with Invalid Checksum : 0
Total Number of VRRP Packets with Unknown Error   : 0
Total Number of VRRP Packets with Invalid VRID    : 0
Console#
```

After network interfaces are configured for the switch, the paths used to send traffic between different interfaces must be set. If routing is enabled on the switch, traffic will automatically be forwarded between all of the local subnetworks. However, to forward traffic to devices on other subnetworks, either configure fixed paths with static routing commands, or enable a dynamic routing protocol that exchanges information with other routers on the network to automatically determine the best path to any subnetwork.

This section includes commands for both static and dynamic routing. These commands are used to connect between different local subnetworks or to connect the router to the enterprise network.

Table 174: IP Routing Commands

Command Group	Function
Global Routing Configuration	Configures global parameters for static and dynamic routing, displays the routing table and statistics for protocols used to exchange routing information
Routing Information Protocol (RIP)	Configures global and interface specific parameters for RIP
Open Shortest Path First (OSPFv2)	Configures global and interface specific parameters for OSPFv2
Open Shortest Path First (OSPFv3)	Configures global and interface specific parameters for OSPFv3
Border Gateway Protocol (BGPv4)	Configures general and neighbor specific parameters for BGPv4
Policy-based Routing for BGP	Configures next-hop routing policies based on criteria defined in various routing parameters

GLOBAL ROUTING CONFIGURATION

Table 175: Global Routing Configuration Commands

Command	Function	Mode
<i>IPv4 Commands</i>		
<code>ip route</code>	Configures static routes	GC
<code>maximum-paths</code>	Sets the maximum number of paths allowed	GC
<code>show ip host-route</code>	Displays the interface associated with known routes	PE
<code>show ip route</code>	Displays specified entries in the routing table	PE
<code>show ip route database</code>	Displays static or dynamically learned entries in the routing table	PE

Table 175: Global Routing Configuration Commands (Continued)

Command	Function	Mode
<code>show ip route summary</code>	Displays summary information for the routing table	PE
<code>show ip traffic</code>	Displays statistics for IP, ICMP, UDP, TCP and ARP protocols	PE
<i>IPv6 Commands</i>		
<code>ipv6 route</code>	Configures static routes	GC
<code>show ipv6 route</code>	Displays specified entries in the routing table	PE

IPv4 Commands

ip route This command configures static routes. Use the **no** form to remove static routes.

SYNTAX

ip route *destination-ip netmask next-hop [distance]*

no ip route {*destination-ip netmask next-hop* | *}

destination-ip – IP address of the destination network, subnetwork, or host.

netmask – Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.

next-hop – IP address of the next hop router used for this route.

distance – An administrative distance indicating that this route can be overridden by dynamic routing information if the distance of the dynamic route is less than that configured for the static route. Note that the default administrative distances used by the dynamic unicast routing protocols is 110 for OSPF, 120 for RIP, 20 for eBGP, and 200 for iBGP. (Range: 1-255, Default: 1)

* – Removes all static routing table entries.

DEFAULT SETTING

No static routes are configured.

COMMAND MODE

Global Configuration

COMMAND USAGE

- ◆ Up to 512 static routes can be configured.
- ◆ Up to eight equal-cost multipaths (ECMP) can be configured for static routing using the `maximum-paths` command.
- ◆ If an administrative distance is defined for a static route, and the same destination can be reached through a dynamic route at a lower administration distance, then the dynamic route will be used.

- ◆ If both static and dynamic paths have the same lowest cost, the first route stored in the routing table, either statically configured or dynamically learned via a routing protocol, will be used.
- ◆ Static routes are included in RIP and OSPF updates periodically sent by the router if this feature is enabled by the RIP or OSPF **redistribute** command (see [page 827](#) or [page 848](#), respectively).

EXAMPLE

This example forwards all traffic for subnet 192.168.1.0 to the gateway router 192.168.5.254, using the default metric of 1.

```
Console(config)#ip route 192.168.1.0 255.255.255.0 192.168.5.254
Console(config)#
```

maximum-paths This command sets the maximum number of paths allowed. Use the **no** form to restore the default settings.

SYNTAX

maximum-paths *path-count*

no maximum-paths

path-count - The maximum number of equal-cost paths to the same destination that can be installed in the routing table. (Range: 1-8)

DEFAULT SETTING

Enabled, 4 paths

COMMAND MODE

Global Configuration

EXAMPLE

```
switch(config)#maximum-paths 8
switch(config)#
```

show ip host-route This command displays the interface associated with known routes.

COMMAND MODE

Privileged Exec

EXAMPLE

```

Console#show ip host-route
  IP Address      MAC Address      VLAN Port
  -----
  192.168.0.99    00-E0-29-94-34-64    1 1/1
  192.168.1.250   00-00-30-01-01-01    3 1/ 1
  10.2.48.2       00-00-30-01-01-02    1 1/ 1
  10.2.5.6        00-00-30-01-01-03    1 1/ 2
  10.3.9.1        00-00-30-01-01-04    2 1/ 3

Console#

```

Table 176: show ip host-route - display description

Field	Description
IP Address	IP address of the destination network, subnetwork, or host.
MAC Address	The physical layer address associated with the IP address.
VLAN	The VLAN that connects to this IP address.
Port	The port that connects to this IP address.

show ip route This command displays information in the Forwarding Information Base (FIB).

SYNTAX

show ip route [**connected** | **database** | **ospf** | **rip** | **static** | **summary**]

bgp – Displays external routes imported from the Border Gateway Protocol (BGP) into this routing domain.

connected – Displays all currently connected entries.

database – All known routes, including inactive routes.

ospf – Displays external routes imported from the Open Shortest Path First (OSPF) protocol into this routing domain.

rip – Displays all entries learned through the Routing Information Protocol (RIP).

static – Displays all static entries.

summary – Displays a brief list of summary information about entries in the routing table, including the maximum number of entries supported, the number of connected routes, the total number of routes currently stored in the routing table, and the number of entries in the FIB.

COMMAND MODE

Privileged Exec

COMMAND USAGE

- ◆ The FIB contains information required to forward IP traffic. It contains the interface identifier and next hop information for each reachable destination

network prefix based on the IP routing table. When routing or topology changes occur in the network, the routing table is updated, and those changes are immediately reflected in the FIB.

The FIB is distinct from the routing table (or, Routing Information Base), which holds all routing information received from routing peers. The forwarding information base contains unique paths only. It does not contain any secondary paths. A FIB entry consists of the minimum amount of information necessary to make a forwarding decision on a particular packet. The typical components within a forwarding information base entry are a network prefix, a router port identifier, and next hop information.

- ◆ This command only displays routes which are currently accessible for forwarding. The router must be able to directly reach the next hop, so the VLAN interface associated with any dynamic or static route entry must be up. Note that routes currently not accessible for forwarding, may still be displayed by using the [show ip route database](#) command.

EXAMPLE

In the following example, note that the entry for RIP displays both the distance and metric for this route.

```

Console#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

R       10.1.1.0/24 [120/2] via 192.168.1.10, VLAN1, 00:00:14
C       127.0.0.0/8 is directly connected, lo
C       192.168.1.0/24 is directly connected, VLAN1
Console#

```

show ip route database This command displays entries in the Routing Information Base (RIB).

COMMAND MODE

Privileged Exec

COMMAND USAGE

The RIB contains all available routes learned through dynamic routing protocols, directly attached networks, and any additionally configured routes such as static routes. The RIB contains the set of all available routes from which optimal entries are selected for use by the Forwarding Information Base (see Command Usage under the [show ip route](#) command).

EXAMPLE

```
Console#show ip route database
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       > - selected route, * - FIB route, p - stale info

C    *> 127.0.0.0/8 is directly connected, lo0
C    *> 192.168.1.0/24 is directly connected, VLAN1

Console#
```

show ip route summary This command displays summary information for the routing table.

COMMAND MODE

Privileged Exec

EXAMPLE

In the following example, the numeric identifier following the named routing table (that is, the Forwarding Information Base) is the FIB ID.

```
Console#show ip route summary
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 8
Connected          2
Total              2
Console#
```

show ip traffic This command displays statistics for IP, ICMP, UDP, TCP and ARP protocols.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip traffic
IP Statistics:
IP received
    4877 total received
        header errors
        unknown protocols
        address errors
        discards
    4763 delivers
        reassembly request datagrams
        reassembled succeeded
        reassembled failed

IP sent
    forwards datagrams
    5927 requests
```



```

discards
no routes
generated fragments
fragment succeeded
fragment failed

ICMP Statistics:
ICMP received
    input
    errors
    destination unreachable messages
    time exceeded messages
    parameter problem message
    echo request messages
    echo reply messages
    redirect messages
    timestamp request messages
    timestamp reply messages
    source quench messages
    address mask request messages
    address mask reply messages

ICMP sent
    output
    errors
    destination unreachable messages
    time exceeded messages
    parameter problem message
    echo request messages
    echo reply messages
    redirect messages
    timestamp request messages
    timestamp reply messages
    source quench messages
    address mask request messages
    address mask reply messages

UDP Statistics:
    2 input
    no port errors
    other errors
    output

TCP Statistics:
    4698 input
    input errors
    5867 output

Console#

```

IPv6 Commands

ipv6 route This command configures static IPv6 routes. Use the **no** form to remove static routes.

SYNTAX

[no] ipv6 route *destination-ipv6-address/prefix-length*
{gateway-address [distance] |

link-local-address%zone-id [*distance*] |
tunnel *interface-number*}

destination-ipv6-address – The IPv6 address of a destination network, subnetwork, or host. This must be a full IPv6 address including the network prefix and host address bits.

prefix-length – A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

gateway-address – IP address of the next hop router used for this route.

link-local-address%zone-id – a link-local address, including a zone-id indicating the VLAN identifier after the % delimiter.

distance – An administrative distance indicating that this route can be overridden by dynamic routing information if the distance of the dynamic route is less than that configured for the static route. Note that the default administrative distances used by the dynamic unicast routing protocols is 110 for OSPF, 120 for RIP, 20 for eBGP, and 200 for iBGP. (Range: 1-255, Default: 1)

interface-number – The number of the outgoing tunnel interface used to reach the destination IPv6 address. (Range: 1-16)
See the [interface tunnel](#) command for more information.

DEFAULT SETTING

No static routes are configured.

COMMAND MODE

Global Configuration

COMMAND USAGE

- ◆ Up to 1K static routes can be configured.
- ◆ Up to eight equal-cost multipaths (ECMP) can be configured for static routing using the [maximum-paths](#) command.
- ◆ If an administrative distance is defined for a static route, and the same destination can be reached through a dynamic route at a lower administration distance, then the dynamic route will be used.
- ◆ The default distance of 1 will take precedence over any other type of route, except for local routes.
- ◆ If both static and dynamic paths have the same lowest cost, the first route stored in the routing table, either statically configured or dynamically learned via a routing protocol, will be used.

- ◆ Static routes are included in RIP and OSPF updates periodically sent by the router if this feature is enabled by the OSPFv3 **redistribute** command (see [page 889](#)).

EXAMPLE

This example forwards all traffic for subnet 2001::/64 to the next hop router 2001:DB8:2222:7272::254, using the default metric of 1.

```
Console(config)#ipv6 route 2001::/64 2001:DB8:2222:7272::254
Console(config)#
```

RELATED COMMANDS

[show ip route summary \(816\)](#)

show ipv6 route This command displays information in the Forwarding Information Base (FIB).

SYNTAX

show ipv6 route [*ipv6-address*[/*prefix-length*]] | **bgp** | **database** | **interface** [**tunnel** *tunnel-number* | **vlan** *vlan-id*] | **local** | **ospf** | **rip** | **static**]

ipv6-address - A full IPv6 address including the network prefix and host address bits.

prefix-length - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

bgp - Displays external routes imported from the Border Gateway Protocol (BGP) into this routing domain.

database - All known routes, including inactive routes.

interface - Displays all routes that be accessed through this interface.

local - Displays all entries for destinations attached directly to this router.

ospf - Displays external routes imported from the Open Shortest Path First (OSPF) protocol into this routing domain.

rip - Displays all entries learned through the Routing Information Protocol (RIP).

static - Displays all static entries.

tunnel-number - Tunnel interface identifier. (Range: 1-16)

vlan-id - VLAN ID. (Range: 1-4094)

COMMAND MODE

Privileged Exec

COMMAND USAGE

- ◆ The FIB contains information required to forward IP traffic. It contains the interface identifier and next hop information for each reachable destination network prefix based on the IP routing table. When routing or topology changes occur in the network, the routing table is updated, and those changes are immediately reflected in the FIB.

The FIB is distinct from the routing table (or, Routing Information Base), which holds all routing information received from routing peers. The forwarding information base contains unique paths only. It does not contain any secondary paths. A FIB entry consists of the minimum amount of information necessary to make a forwarding decision on a particular packet. The typical components within a forwarding information base entry are a network prefix, a router port identifier, and next hop information.

- ◆ This command only displays routes which are currently accessible for forwarding. The router must be able to directly reach the next hop, so the VLAN interface associated with any dynamic or static route entry must be up.

EXAMPLE

In the following example, note that the last entry displays both the distance and metric for this route.

```
Console#show ipv6 route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
C      ::1/128, lo0
?      FE80::/64, VLAN1 inactive
C      FE80::/64, VLAN1
?      FF00::/8, VLAN1 inactive
O IA   3FFF:1::/32 [110/3]
       via FE80::204:FF:FE05:6, VLAN1

Console#
```

ROUTING INFORMATION PROTOCOL (RIP)

Table 177: Routing Information Protocol Commands

Command	Function	Mode
<code>router rip</code>	Enables the RIP routing protocol	GC
<code>default-information originate</code>	Generates a default external route into an autonomous system	RC
<code>default-metric</code>	Sets the default metric assigned to external routes imported from other protocols	RC
<code>distance</code>	Defines an administrative distance for external routes learned from other routing protocols	RC
<code>maximum-prefix</code>	Sets the maximum number of RIP routes allowed	RC
<code>neighbor</code>	Defines a neighboring router with which to exchange information	RC
<code>network</code>	Specifies the network interfaces that are to use RIP routing	RC
<code>passive-interface</code>	Stops RIP from sending routing updates on the specified interface	RC
<code>redistribute</code>	Redistribute routes from one routing domain to another	RC
<code>timers basic</code>	Sets basic timers, including update, timeout, garbage collection	RC
<code>version</code>	Specifies the RIP version to use on all network interfaces (if not already specified with a receive version or send version command)	RC
<code>ip rip authentication mode</code>	Specifies the type of authentication used for RIP2 packets	IC
<code>ip rip authentication string</code>	Enables authentication for RIP2 packets and specifies keys	IC
<code>ip rip receive version</code>	Sets the RIP receive version to use on a network interface	IC
<code>ip rip receive-packet</code>	Configures the interface to receive of RIP packets	IC
<code>ip rip send version</code>	Sets the RIP send version to use on a network interface	IC
<code>ip rip send-packet</code>	Configures the interface to send RIP packets	IC
<code>ip rip split-horizon</code>	Enables split-horizon or poison-reverse loop prevention	IC
<code>clear ip rip route</code>	Clears specified data from the RIP routing table	PE
<code>show ip protocols rip</code>	Displays RIP process parameters	PE
<code>show ip rip</code>	Displays information about RIP routes and configuration settings	PE

router rip This command enables Routing Information Protocol (RIP) routing for all IP interfaces on the router. Use the **no** form to disable it.

SYNTAX

[no] router rip

COMMAND MODE

Global Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

- ◆ RIP is used to specify how routers exchange routing table information.
- ◆ This command is also used to enter router configuration mode.

EXAMPLE

```
Console(config)#router rip
Console(config-router)#
```

RELATED COMMANDS

[network \(826\)](#)

default-information originate This command generates a default external route into the local RIP autonomous system. Use the **no** form to disable this feature.

SYNTAX

[no] default-information originate

DEFAULT SETTING

Disabled

COMMAND MODE

Router Configuration

COMMAND USAGE

This command sets a default route for every Layer 3 interface where RIP is enabled. The response packet to external queries marks each active RIP interface as a default router with the IP address 0.0.0.0.

EXAMPLE

```
Console(config-router)#default-information originate
Console(config-router)#
```

RELATED COMMANDS

[ip route \(812\)](#)
[redistribute \(827\)](#)

default-metric This command sets the default metric assigned to external routes imported from other protocols. Use the **no** form to restore the default value.

SYNTAX

default-metric *metric-value*

no default-metric

metric-value – Metric assigned to external routes. (Range: 1-15)

DEFAULT SETTING

1

COMMAND MODE

Router Configuration

COMMAND USAGE

- ◆ This command does not override the metric value set by the [redistribute](#) command. When a metric value has not been configured by the [redistribute](#) command, the **default-metric** command sets the metric value to be used for all imported external routes.
- ◆ The default metric must be used to resolve the problem of redistributing external routes with incompatible metrics.
- ◆ It is advisable to use a low metric when redistributing routes from another protocol into RIP. Using a high metric limits the usefulness of external routes redistributed into RIP. For example, if a metric of 10 is defined for redistributed routes, these routes can only be advertised to routers up to 5 hops away, at which point the metric exceeds the maximum hop count of 15. By defining a low metric of 1, traffic can follow a imported route the maximum number of hops allowed within a RIP domain. However, note that using a low metric can increase the possibility of routing loops For example, this can occur if there are multiple redistribution points and the router learns about the same external network with a better metric from a redistribution point other than that derived from the original source.

EXAMPLE

This example sets the default metric to 5.

```
Console(config-router)#default-metric 5
Console(config-router)#
```

RELATED COMMANDS

[redistribute \(827\)](#)

distance This command defines an administrative distance for external routes learned from other routing protocols. Use the **no** form to restore the default setting.

SYNTAX

[no] distance *distance network-address netmask [acl-name]*

distance - Administrative distance for external routes. External routes are routes for which the best path is learned from a neighbor external to the local RIP autonomous system. Routes with a distance of 255 are not installed in the routing table.

(Range: 1-255)

network-address - IP address of a route entry.

netmask - Network mask for the route. This mask identifies the network address bits used for the associated routing entries.

acl-name - Name of the access control list. Any type of ACL can be specified, including standard or extended IP ACLs and MAC ACLs.

(Range: 1-16 characters)

DEFAULT SETTING

None

COMMAND MODE

Router Configuration

COMMAND USAGE

- ◆ Administrative distance is used by the routers to select the preferred path when there are two or more different routes to the same destination from two different routing protocols. A smaller administrative distance indicates a more reliable protocol.
- ◆ An access list can be used to filter networks according to the IP address of the router supplying the routing information. For example, to filter out unreliable routing information from routers not under your administrative control.
- ◆ The administrative distance is applied to all routes learned for the specified network.

EXAMPLE

```
Console(config-router)#distance 2 192.168.3.0 255.255.255.0
Console(config-router)#
```


maximum-prefix This command sets the maximum number of RIP routes allowed by the system. Use the **no** form to restore the default setting.

SYNTAX

maximum-prefix *maximum-routes*

no maximum-prefix

maximum-routes - The maximum number of RIP routes which can be installed in the routing table. (Range: 1-7168)

DEFAULT SETTING

1024

COMMAND MODE

Router Configuration

COMMAND USAGE

All the learned RIP routes may not be copied to the hardware tables in ASIC for fast data forwarding because of hardware resource limitations.

EXAMPLE

```
Console(config-router)#maximum-prefix 1024
Console(config-router)#
```

neighbor This command defines a neighboring router with which this router will exchange routing information. Use the **no** form to remove an entry.

SYNTAX

[no] neighbor *ip-address*

ip-address - IP address of a neighboring router.

DEFAULT SETTING

No neighbors are defined.

COMMAND MODE

Router Configuration

COMMAND USAGE

- ◆ This command can be used to configure a static neighbor (specifically for point-to-point links) with which this router will exchange routing information, rather than relying on broadcast or multicast messages generated by the RIP protocol.
- ◆ Use this command in conjunction with the [passive-interface](#) command to control the routing updates sent to specific neighbors.

EXAMPLE

```
Console(config-router)#neighbor 10.2.0.254  
Console(config-router)#
```

RELATED COMMANDS

[passive-interface \(827\)](#)

network This command specifies the network interfaces that will be included in the RIP routing process. Use the **no** form to remove an entry.

SYNTAX

[no] network {*ip-address netmask* | **vlan** *vlan-id*}

ip-address – IP address of a network directly connected to this router.

netmask - Network mask for the route. This mask identifies the network address bits used for the associated routing entries.

vlan-id - VLAN ID. (Range: 1-4094)

DEFAULT SETTING

No networks are specified.

COMMAND MODE

Router Configuration

COMMAND USAGE

RIP only sends and receives updates on interfaces specified by this command. If a network is not specified, the interfaces in that network will not be advertised in any RIP updates.

EXAMPLE

This example includes network interface 10.1.0.0 in the RIP routing process.

```
Console(config-router)#network 10.1.0.0  
Console(config-router)#
```

RELATED COMMANDS

[router rip \(822\)](#)

passive-interface This command stops RIP from sending routing updates on the specified interface. Use the **no** form to disable this feature.

SYNTAX

[no] passive-interface vlan *vlan-id*
vlan-id - VLAN ID. (Range: 1-4094)

DEFAULT SETTING

Disabled

COMMAND MODE

Router Configuration

COMMAND USAGE

- ◆ If this command is used to stop sending routing updates on an interface, the attached subnet will still continue to be advertised to other interfaces, and updates from other routers on that interface will continue to be received and processed.
- ◆ Use this command in conjunction with the [neighbor](#) command to control the routing updates sent to specific neighbors.

EXAMPLE

```
Console(config-router)#passive-interface vlan1
Console(config-router)#
```

RELATED COMMANDS

[neighbor \(825\)](#)

redistribute This command imports external routing information from other routing domains (that is, directly connected routes, protocols, or static routes) into the autonomous system. Use the **no** form to disable this feature.

SYNTAX

[no] redistribute (bgp | connected | ospf | static) [metric *metric-value*

bgp – Displays external routes imported from the Border Gateway Protocol (BGP) into this routing domain.

connected - Imports routes that are established automatically just by enabling IP on an interface.

ospf - External routes will be imported from the Open Shortest Path First (OSPF) protocol into this routing domain.

static - Static routes will be imported into this routing domain.

metric-value - Metric value assigned to all external routes for the specified protocol. (Range: 1-16)

DEFAULT SETTING

redistribution - none

metric-value - set by the [default-metric](#) command

COMMAND MODE

Router Configuration

COMMAND USAGE

- ◆ When a metric value has not been configured by the **redistribute** command, the [default-metric](#) command sets the metric value to be used for all imported external routes.
- ◆ A route metric must be used to resolve the problem of redistributing external routes with incompatible metrics.
- ◆ It is advisable to use a low metric when redistributing routes from another protocol into RIP. Using a high metric limits the usefulness of external routes redistributed into RIP. For example, if a metric of 10 is defined for redistributed routes, these routes can only be advertised to routers up to 5 hops away, at which point the metric exceeds the maximum hop count of 15. By defining a low metric of 1, traffic can follow a imported route the maximum number of hops allowed within a RIP domain. However, using a low metric can increase the possibility of routing loops. For example, this can occur if there are multiple redistribution points and the router learns about the same external network with a better metric from a redistribution point other than that derived from the original source.

EXAMPLE

This example redistributes routes learned from OSPF and sets the metric for all external routes imported from OSPF to a value of 3.

```
Console(config-router)#redistribute ospf metric 3
Console(config-router)#
```

This example redistributes static routes and sets the metric for all of these routes to a value of 3.

```
Console(config-router)#redistribute static metric 3
Console(config-router)#
```

RELATED COMMANDS

[default-metric \(823\)](#)

timers basic This command configures the RIP update timer, timeout timer, and garbage-collection timer. Use the **no** form to restore the defaults.

SYNTAX

timers basic *update timeout garbage*

no timers basic

update – Sets the update timer to the specified value.
(Range: 5-2147483647 seconds)

timeout – Sets the timeout timer to the specified value. (Range: 90-360 seconds)

garbage – Sets the garbage collection timer to the specified value.
(Range: 60-240 seconds)

DEFAULT SETTING

Update: 30 seconds

Timeout: 180 seconds

Garbage collection: 120 seconds

COMMAND MODE

Router Configuration

COMMAND USAGE

- ◆ The *update* timer sets the rate at which updates are sent. This is the fundamental timer used to control all basic RIP processes.
- ◆ The *timeout* timer is the time after which there have been no update messages that a route is declared dead. The route is marked inaccessible (i.e., the metric set to infinite) and advertised as unreachable. However, packets are still forwarded on this route.
- ◆ After the *timeout* interval expires, the router waits for an interval specified by the *garbage-collection* timer before removing this entry from the routing table. This timer allows neighbors to become aware of an invalid route prior to it being purged by this device.
- ◆ Setting the update timer to a short interval can cause the router to spend an excessive amount of time processing updates.
- ◆ These timers must be set to the same values for all routers in the network.

EXAMPLE

This example sets the update timer to 40 seconds. The timeout timer is subsequently set to 240 seconds, and the garbage-collection timer to 160 seconds.

```
Console(config-router)#timers basic 15
Console(config-router)#
```

version This command specifies a RIP version used globally by the router. Use the **no** form to restore the default value.

SYNTAX

version {1 | 2}

no version

1 - RIP Version 1

2 - RIP Version 2

DEFAULT SETTING

Receive: Accepts RIPv1 or RIPv2 packets

Send: Route information is broadcast to other routers with RIPv2.

COMMAND MODE

Router Configuration

COMMAND USAGE

- ◆ When this command is used to specify a global RIP version, any VLAN interface not previously set by the [ip rip receive version](#) or [ip rip send version](#) command will use the global RIP version setting.
- ◆ When the **no** form of this command is used to restore the default value, any VLAN interface not previously set by the [ip rip receive version](#) or [ip rip send version](#) command will be set to the default send or receive version.
- ◆ Any configured interface settings take precedence over the global settings.

EXAMPLE

This example sets the global version for RIP to send and receive version 2 packets.

```
Console(config-router)#version 2
Console(config-router)#
```

RELATED COMMANDS

[ip rip receive version \(832\)](#)

[ip rip send version \(834\)](#)

ip rip authentication mode This command specifies the type of authentication that can be used for RIPv2 packets. Use the **no** form to restore the default value.

SYNTAX

ip rip authentication mode {md5 | text}

no ip rip authentication mode

md5 - Message Digest 5 (MD5) authentication

text - Indicates that a simple password will be used.

DEFAULT SETTING

Text authentication

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- ◆ The password to be used for authentication is specified in the [ip rip authentication string](#) command.
- ◆ This command requires the interface to exchange routing information with other routers based on an authorized password. (Note that this command only applies to RIPv2.)
- ◆ For authentication to function properly, both the sending and receiving interface must be configured with the same password or authentication key.
- ◆ MD5 is a one-way hash algorithm that takes the authentication key and produces a 128 bit message digest or “fingerprint.” This makes it computationally infeasible to produce two messages having the same message digest, or to produce any message having a given pre-specified target message digest.

EXAMPLE

This example sets the authentication mode to plain text.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip authentication mode text
Console(config-if)#
```

RELATED COMMANDS

[ip rip authentication string \(832\)](#)

ip rip authentication string This command specifies an authentication key for RIPv2 packets. Use the **no** form to delete the authentication key.

SYNTAX

ip rip authentication string *key-string*

no ip rip authentication string

key-string - A password used for authentication.
(Range: 1-16 characters, case sensitive)

DEFAULT SETTING

No authentication key

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- ◆ This command can be used to restrict the interfaces that can exchange RIPv2 routing information. (Note that this command does not apply to RIPv1.)
- ◆ For authentication to function properly, both the sending and receiving interface must be configured with the same password, and authentication enabled by the [ip rip authentication mode](#) command.

EXAMPLE

This example sets an authentication password of “small” to verify incoming routing messages and to tag outgoing routing messages.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip authentication string small
Console(config-if)#
```

RELATED COMMANDS

[ip rip authentication mode \(831\)](#)

ip rip receive version This command specifies a RIP version to receive on an interface. Use the **no** form to restore the default value.

SYNTAX

ip rip receive version {1 | 2}

no ip rip receive version

- 1** - Accepts only RIPv1 packets.
- 2** - Accepts only RIPv2 packets.

DEFAULT SETTING

RIPv1 or RIPv2 packets

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- ◆ Use this command to override the global setting specified by the RIP [version](#) command.
- ◆ You can specify the receive version based on these options:
 - Use version 1 or version 2 if all routers in the local network are based on RIPv1 or RIPv2, respectively.
 - Use the default of version 1 or 2 if some routers in the local network are using RIPv2, but there are still some older routers using RIPv1.

EXAMPLE

This example sets the interface version for VLAN 1 to receive RIPv1 packets.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip receive version 1
Console(config-if)#
```

RELATED COMMANDS

[version \(830\)](#)

ip rip receive-packet This command configures the interface to receive RIP packets. Use the **no** form to disable this feature.

SYNTAX

[no] ip rip receive-packet

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

Enabled

COMMAND USAGE

Use the **no** form of this command if it is not required to add any dynamic entries to the routing table for an interface. For example, when only static routes are to be allowed for a specific interface.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ip rip receive-packet
Console(config-if)#
```

RELATED COMMANDS

[ip rip send-packet \(835\)](#)

ip rip send version This command specifies a RIP version to send on an interface. Use the **no** form to restore the default value.

SYNTAX

ip rip send version {1 | 2 | 1-compatible}

no ip rip send version

1 - Sends only RIPv1 packets.

2 - Sends only RIPv2 packets.

1-compatible - Route information is broadcast to other routers with RIPv2.

DEFAULT SETTING

1-compatible (Route information is broadcast to other routers with RIPv2)

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- ◆ Use this command to override the global setting specified by the RIP [version](#) command.
- ◆ You can specify the send version based on these options:
 - Use version 1 or version 2 if all routers in the local network are based on RIPv1 or RIPv2, respectively.
 - Use “1-compatible” to propagate route information by broadcasting to other routers on the network using RIPv2, instead of multicasting as normally required by RIPv2. (Using this mode allows older RIPv2 routers which only receive RIP broadcast messages to receive all of the information provided by RIPv2, including subnet mask, next hop and authentication information.)

EXAMPLE

This example sets the interface version for VLAN 1 to send RIPv1 packets.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip send version 1
Console(config-if)#
```

RELATED COMMANDS

[version \(830\)](#)

ip rip send-packet This command configures the interface to send RIP packets. Use the **no** form to disable this feature.

[no] ip rip send-packet

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

Enabled

COMMAND USAGE

The **no** form of this command allows the router to passively monitor route information advertised by other routers attached to the network, without transmitting any RIP updates.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ip rip send-packet
Console(config-if)#
```

RELATED COMMANDS

[ip rip receive-packet \(833\)](#)

ip rip split-horizon This command enables split-horizon or poison-reverse (a variation) on an interface. Use the **no** form to disable this function.

SYNTAX

ip rip split-horizon [poisoned]

no rip ip split-horizon

poisoned - Enables poison-reverse on the current interface.

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

split-horizon poisoned

COMMAND USAGE

- ◆ Split horizon never propagates routes back to an interface from which they have been acquired.
- ◆ Poison reverse propagates routes back to an interface port from which they have been acquired, but sets the distance-vector metrics to infinity. (This provides faster convergence.)
- ◆ If split-horizon is disabled with the **no rip ip split-horizon** command, and a loop occurs, the hop count for a route may be gradually incremented to infinity (that is, 16) before the route is deemed unreachable.

EXAMPLE

This example propagates routes back to the source using poison-reverse.

```
Console(config)#interface vlan 1
Console(config-if)#ip split-horizon poison-reverse
Console(config-if)#
```

clear ip rip route This command clears specified data from the RIP routing table.

SYNTAX

clear ip rip route {ip-address netmask | all | connected | ospf | rip | static}

ip-address - IP address of a route entry.

netmask - Network mask for the route. This mask identifies the network address bits used for the associated routing entries.

all - Deletes all entries from the routing table.

connected - Deletes all currently connected entries.

ospf - Deletes all entries learned through the Open Shortest Path First routing protocol.

rip - Deletes all entries learned through the Routing Information Protocol.

static - Deletes all static entries.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

Using this command with the “all” parameter clears the RIP table of all routes. To avoid deleting the entire RIP network, use the **redistribute connected** command to make the RIP network a connected route. To delete the RIP routes learned from neighbors and also keep the RIP network intact, use the “rip” parameter with this command (**clear ip rip route rip**).

EXAMPLE

This example clears one specific route.

```
Console#clear ip rip route 192.168.1.0 255.255.255.0
Console#
```

show ip protocols rip This command displays RIP process parameters.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip protocols rip
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-5 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing:
  Default version control: send version by interface set, receive version by
  interface set
    Interface  Send      Recv
    VLAN1      1-compatible 1 2
  Routing for Networks:
    10.0.0.0/24
  Routing Information Sources:
    Gateway         Distance  Last Update  Bad Packets  Bad Routes
    10.0.0.2         120      00:00:13     0            0
  The maximum number of RIP routes allowed: 7872
```

```
Distance: Default is 120
Console#
```

show ip rip This command displays information about RIP routes and configuration settings. Use this command without any keywords to display all RIP routes.

SYNTAX

show ip rip [**interface** **vlan** *vlan-id*]

interface - Shows RIP configuration settings for all interfaces or for a specified interface.

vlan-id - VLAN ID. (Range: 1-4094)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip rip
```

```
Codes: R - RIP, Rc - RIP connected, Rs - RIP static,
       C - Connected, S - Static, O - OSPF
```

Network	Next Hop	Metric	From	Interface	Time
Rc 192.168.0.0/24		1		VLAN1	01:57

```
Console#show ip rip interface vlan 1
```

```
Interface: vlan1
```

```
Routing Protocol: RIP
```

```
Receive RIPv1 and RIPv2 packets
```

```
Send RIPv1 Compatible
```

```
Passive interface: Disabled
```

```
Authentication mode: (None)
```

```
Authentication string: (None)
```

```
Split horizon: Enabled with Poisoned Reverse
```

```
IP interface address: 192.168.0.2/24
```

```
Console#
```

OPEN SHORTEST PATH FIRST (OSPFv2)

Table 178: Open Shortest Path First Commands

Command	Function	Mode
<i>General Configuration</i>		
<code>router ospf</code>	Enables or disables OSPFv2	GC
<code>compatible rfc1583</code>	Calculates summary route costs using RFC 1583 (early OSPFv2)	RC
<code>default-information originate</code>	Generates a default external route into an autonomous system	RC
<code>router-id</code>	Sets the router ID for this device	RC
<code>timers spf</code>	Configures the delay after a topology change and the hold time between consecutive SPF calculations	RC
<code>clear ip ospf process</code>	Clears and restarts the OSPF routing process	PE
<i>Route Metrics and Summaries</i>		
<code>area default-cost</code>	Sets the cost for a default summary route sent into a stub or NSSA	RC
<code>area range</code>	Summarizes routes advertised by an ABR	RC
<code>auto-cost reference-bandwidth</code>	Calculates default metrics for an interface based on bandwidth	RC
<code>default-metric</code>	Sets the default metric for external routes imported from other protocols	RC
<code>redistribute</code>	Redistribute routes from one routing domain to another	RC
<code>summary-address</code>	Summarizes routes advertised by an ASBR	RC
<i>Area Configuration</i>		
<code>area nssa</code>	Defines a not-so-stubby that can import external routes	RC
<code>area stub</code>	Defines a stubby area that cannot send or receive LSAs	RC
<code>area virtual-link</code>	Defines a virtual link from an area border routers to the backbone	RC
<code>network area</code>	Assigns specified interface to an area	RC
<i>Interface Configuration</i>		
<code>ip ospf authentication</code>	Specifies the authentication type for an interface	IC
<code>ip ospf authentication-key</code>	Assigns a simple password to be used by neighboring routers	IC
<code>ip ospf cost</code>	Specifies the cost of sending a packet on an interface	IC
<code>ip ospf dead-interval</code>	Sets the interval at which hello packets are not seen before neighbors declare the router down	IC
<code>ip ospf hello-interval</code>	Specifies the interval between sending hello packets	IC
<code>ip ospf message-digest-key</code>	Enables MD5 authentication and sets the key for an interface	IC
<code>ip ospf priority</code>	Sets the router priority used to determine the designated router	IC

Table 178: Open Shortest Path First Commands (Continued)

Command	Function	Mode
<code>ip ospf retransmit-interval</code>	Specifies the time between resending a link-state advertisement	IC
<code>ip ospf transmit-delay</code>	Estimates time to send a link-state update packet over an interface	IC
<code>passive-interface</code>	Suppresses OSPF routing traffic on the specified interface	RC
<i>Display Information</i>		
<code>show ip ospf</code>	Displays general information about the routing processes	PE
<code>show ip ospf border-routers</code>	Displays routing table entries for Area Border Routers (ABR) and Autonomous System Boundary Routers (ASBR)	PE
<code>show ip ospf database</code>	Shows information about different LSAs in the database	PE
<code>show ip ospf interface</code>	Displays interface information	PE
<code>show ip ospf neighbor</code>	Displays neighbor information	PE
<code>show ip ospf route</code>	Displays the OSPF routing table	PE
<code>show ip ospf virtual-links</code>	Displays parameters and the adjacency state of virtual links	PE
<code>show ip protocols ospf</code>	Displays OSPF process parameters	PE

General Configuration

router ospf This command enables Open Shortest Path First (OSPFv2) routing for all IP interfaces on the router and enters router configuration mode. Use the **no** form to disable OSPF for all processes or for a specified process.

SYNTAX

[no] router ospf *[process-id]*

process-id - Process ID must be entered when configuring multiple routing instances. (Range: 1-65535; Default: 1)

COMMAND MODE

Global Configuration

DEFAULT SETTING

No routing process is defined.

COMMAND USAGE

- ◆ OSPF is used to specify how routers exchange routing table information.
- ◆ This command is also used to enter router configuration mode.
- ◆ If the process ID is not defined, the default is instance 1.

EXAMPLE

```
Console(config)#router ospf
Console(config-router)#
```

RELATED COMMANDS

[network area \(856\)](#)

compatible rfc1583 This command calculates summary route costs using RFC 1583 (early OSPFv2). Use the **no** form to calculate costs using RFC 2328 (OSPFv2).

SYNTAX

[no] compatible rfc1583

COMMAND MODE

Router Configuration

DEFAULT SETTING

RFC 1583 compatible

COMMAND USAGE

- ◆ When RFC 1583 compatibility is enabled, only cost is used when choosing among multiple AS-external LSAs advertising the same destination. When disabled, preference is based on type of path (where type 1 external paths are preferred over type 2 external paths, using cost only to break ties (RFC 2328).
- ◆ All routers in an OSPF routing domain should use the same RFC for calculating summary routes.
- ◆ If there are any OSPF routers in an area exchanging summary information (specifically, ABRs) which have not been upgraded to OSPFv2, this command should be used on the newly upgraded OSPFv2 routers to ensure compatibility with routers still running older OSPFv2 code. Once all systems have been upgraded to newer OSPFv2 code, use the no form of this command to restore compatibility for all systems with RFC 2328.

EXAMPLE

```
Console(config-router)#compatible rfc1583
Console(config-router)#
```

default-information originate This command generates a default external route into an autonomous system. Use the **no** form to disable this feature.

SYNTAX

default-information originate [**always**] [**metric** *interface-metric*] [**metric-type** *metric-type*]

no default-information originate [**always** | **metric** | **metric-type**]

always - Always advertise itself as a default external route for the local AS regardless of whether the router has a default route. (See ["ip route" on page 812.](#))

interface-metric - Metric assigned to the default route. (Range: 0-16777214)

metric-type - External link type used to advertise the default route.
(Options: Type 1, Type 2)

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

Metric: 20

Metric Type: 2

COMMAND USAGE

- ◆ If the **always** parameter is not selected, the router can only advertise a default external route into the AS if it has been configured to import external routes through other routing protocols or static routing, and such a route is known. (See the [redistribute](#) command.)
- ◆ The metric for the default external route is used to calculate the path cost for traffic passed from other routers within the AS out through the ASBR.
- ◆ When you use this command to redistribute routes into a routing domain (i.e., an Autonomous System, this router automatically becomes an Autonomous System Boundary Router (ASBR). However, an ASBR does not, by default, generate a default route into the routing domain.
 - If you use the **always** keyword, the router will advertise itself as a default external route into the AS, even if a default external route does not actually exist. To define a default route, use the [ip route](#) command.
 - If you do *not* use the **always** keyword, the router can only advertise a default external route into the AS if the [redistribute](#) command is used to import external routes via RIP or static routing, and such a route is known.
- ◆ Type 1 route advertisements add the internal cost to the external route metric. Type 2 routes do not add the internal cost metric. When comparing Type 2

routes, the internal cost is only used as a tie-breaker if several Type 2 routes have the same cost.

- ◆ This command should not be used to generate a default route for a stub or NSSA. To generate a default route for these area types, use the [area stub](#) or [area nssa](#) commands.

EXAMPLE

This example assigns a metric of 20 to the default external route advertised into an autonomous system, sending it as a Type 2 external metric.

```
Console(config-router)#default-information originate metric 20 metric-type 2
Console(config-router)#
```

RELATED COMMANDS

[ip route \(812\)](#)
[redistribute \(889\)](#)

router-id This command assigns a unique router ID for this device within the autonomous system for the current OSPF process. Use the **no** form to use the default router identification method (i.e., the highest interface address).

SYNTAX

router-id *ip-address*

no router-id

ip-address - Router ID formatted as an IPv4 address.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Highest interface address

COMMAND USAGE

- ◆ This command sets the router ID for the OSPF process specified in the [router ospf](#) command.
- ◆ The router ID must be unique for every router in the autonomous system. Using the default setting based on the highest interface address ensures that each router ID is unique. (Note that the router ID can also be set to 0.0.0.0 or 255.255.255.255).
- ◆ If this router already has registered neighbors, the new router ID will be used when the router is rebooted, or manually restarted by entering the **no router ospf** followed by the **router ospf** command.

- ◆ If the priority values of the routers bidding to be the designated router or backup designated router for an area are equal, the router with the highest ID is elected.

EXAMPLE

```
Console(config-router)#router-id 10.1.1.1  
Console(config-router)#
```

RELATED COMMANDS

[router ospf \(840\)](#)

timers spf This command configures the delay after receiving a topology change and starting the shortest path first (SPF) calculation, and the hold time between making two consecutive SPF calculations. Use the **no** form to restore the default values.

SYNTAX

timers spf *spf-delay spf-holdtime*

no timers spf

spf-delay - The delay after receiving a topology change notification and starting the SPF calculation. (Range: 0-2147483647 seconds)

spf-holdtime - Minimum time between two consecutive SPF calculations. (Range: 0-2147483647 seconds)

COMMAND MODE

Router Configuration

DEFAULT SETTING

SPF delay: 5 seconds

SPF holdtime: 10 seconds

COMMAND USAGE

- ◆ Setting the SPF holdtime to 0 means that there is no delay between consecutive calculations.
- ◆ Using a low value allows the router to switch to a new path faster, but uses more CPU processing time.

EXAMPLE

```
Console(config-router)#timers spf 20  
Console(config-router)#
```

clear ip ospf process This command clears and restarts the OSPF routing process. Specify the process ID to clear a particular OSPF process. When no process ID is specified, this command clears all running OSPF processes.

SYNTAX

clear ip ospf [*process-id*] **process**

process-id - Specifies the routing process ID. (Range: 1-65535)

DEFAULT SETTING

Clears all routing processes.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#clear ip ospf process
Console#
```

Route Metrics and Summaries

area default-cost This command specifies a cost for the default summary route sent into a stub or NSSA from an Area Border Router (ABR). Use the **no** form to remove the assigned default cost.

SYNTAX

area *area-id* **default-cost** *cost*

no area *area-id* **default-cost**

area-id - Identifies the stub or NSSA. (The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.)

cost - Cost for the default summary route sent to a stub or NSSA. (Range: 0-16777215)

COMMAND MODE

Router Configuration

DEFAULT SETTING

Default cost: 1

COMMAND USAGE

- ◆ If the default cost is set to "0," the router will not advertise a default route into the attached stub or NSSA.

EXAMPLE

```
Console(config-router)#area 10.3.9.0 default-cost 10  
Console(config-router)#
```

RELATED COMMANDS

[area stub \(852\)](#)

[area nssa \(851\)](#)

area range This command summarizes the routes advertised by an Area Border Router (ABR). Use the **no** form to disable this function.

SYNTAX

[no] area area-id range ip-address netmask [advertise | not-advertise]

area-id - Identifies an area for which the routes are summarized. The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.

ip-address - Base address for the routes to summarize.

netmask - Network mask for the summary route.

advertise - Advertises the specified address range.

not-advertise - The summary is not sent, and the routes remain hidden from the rest of the network.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

- ◆ This command can be used to summarize intra-area routes and advertise this information to other areas through Area Border Routers (ABRs).
- ◆ If the network addresses within an area are assigned in a contiguous manner, the ABRs can advertise a summary route that covers all of the individual networks within the area that fall into the specified range using a single **area range** command.
- ◆ If routes are set to be advertised by this command, the router will issue a Type 3 summary LSA for each address range specified by this command.
- ◆ This router supports up to 64 summary routes for area ranges.

EXAMPLE

This example creates a summary address for all area routes in the range of 10.2.x.x.

```
Console(config-router)#area 10.2.0.0 range 10.2.0.0 255.255.0.0 advertise
Console(config-router)#
```

auto-cost reference-bandwidth

Use this command to calculate the default metrics for an interface based on bandwidth. Use the **no** form to automatically assign costs based on interface type.

SYNTAX

auto-cost reference-bandwidth *reference-value*

no auto-cost reference-bandwidth

reference-value - Bandwidth of interface. (Range: 1-4294967 Mbps)

COMMAND MODE

Router Configuration

DEFAULT SETTING

1 Mbps

COMMAND USAGE

- ◆ The system calculates the cost for an interface by dividing the reference bandwidth by the interface bandwidth. By default, the cost is 1 Mbps for all port types (including 100 Mbps ports, 1 Gigabit ports, and 10 Gigabit ports).
- ◆ A higher reference bandwidth can be used for aggregate links to indicate preferred use as a lower cost interface.
- ◆ The [ip ospf cost](#) command overrides the cost calculated by the **auto-cost reference-bandwidth** command.

EXAMPLE

This example sets the reference value to 10000, which generates a cost of 100 for 100 Mbps ports, 10 for 1 Gbps ports and 1 for 10 Gbps ports.

```
Console(config-router)#auto-cost reference-bandwidth 10000
Console(config-router)#
```

RELATED COMMANDS

[ip ospf cost \(860\)](#)

default-metric This command sets the default metric for external routes imported from other protocols. Use the **no** form to remove the default metric for the supported protocol types.

SYNTAX

default-metric *metric-value*

no default-metric

metric-value – Metric assigned to all external routes imported from other protocols. (Range: 0-16777214)

COMMAND MODE

Router Configuration

DEFAULT SETTING

20

COMMAND USAGE

- ◆ The default metric must be used to resolve the problem of redistributing external routes from other protocols that use incompatible metrics.
- ◆ This command does not override the metric value set by the **redistribute** command. When a metric value has not been configured by the **redistribute** command, the **default-metric** command sets the metric value to be used for all imported external routes.

EXAMPLE

```
Console(config-router)#default-metric 100
Console(config-router)#
```

RELATED COMMANDS

redistribute (848)

redistribute This command redistributes external routing information from other routing protocols and static routes into an autonomous system. Use the **no** form to disable this feature or to restore the default settings.

SYNTAX

redistribute {**bgp** | **connected** | **rip** | **static**} [**metric** *metric-value*]
[**metric-type** *type-value*] [**tag** *tag-value*]

no redistribute {**connected** | **rip** | **static**} [**metric**] [**metric-type**] [**tag**]

bgp – Displays external routes imported from the Border Gateway Protocol (BGP) into this routing domain.

connected - Imports all currently connected entries.

rip - Imports entries learned through the Routing Information Protocol.

static - Static routes will be imported into this Autonomous System.

metric-value - Metric assigned to all external routes for the specified protocol. (Range: 0-16777214; Default: 10)

type-value

1 - Type 1 external route

2 - Type 2 external route (default) - Routers do not add internal route metric to external route metric.

tag-value - A tag placed in the AS-external LSA to identify a specific external routing domain, or to pass additional information between routers. (Range: 0-4294967295)

COMMAND MODE

Router Configuration

DEFAULT SETTING

redistribution - none

metric-value - 10

type-metric - 2

COMMAND USAGE

- ◆ This command is used to import routes learned from other routing protocols into the OSPF domain, and to generate AS-external-LSAs.
- ◆ When you redistribute external routes into an OSPF autonomous system (AS), the router automatically becomes an autonomous system boundary router (ASBR). If the **redistribute** command is used in conjunction with the **default-information originate** command to generate a “default” external route into the AS, the metric value specified in this command supersedes the metric specified in the **default-information originate** command.
- ◆ Metric type specifies the way to advertise routes to destinations outside the AS through External LSAs. When a Type 1 LSA is received by a router, it adds the internal cost to the external route metric. In other words, the cost of the route from any router within the AS is equal to the cost associated with reaching the advertising ASBR, plus the cost of the external route. When a Type 2 LSA is received by a router, it only uses the external route metric to determine route cost.
- ◆ A tag can be used to distinguish between routes learned from different external autonomous systems (other routing protocols). For example, if there are two ASBRs in a routing domain: A and B. ASBR A can be configured to redistribute routes learned from RIP domain 1 (identified by tag 1) and ASBR B can redistribute routes learned from RIP domain 2 (identified by tag 2).

EXAMPLE

This example redistributes routes learned from RIP as Type 1 external routes.

```
Console(config-router)#redistribute rip metric-type 1  
Console(config-router)#
```

RELATED COMMANDS

[default-information originate \(842\)](#)

summary-address This command aggregates routes learned from other protocols. Use the **no** form to remove a summary address.

SYNTAX

[no] summary-address *summary-address netmask*

summary-address - Summary address covering a range of addresses.

netmask - Network mask for the summary route.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

Redistributing routes from other protocols into OSPF normally requires the router to advertise each route individually in an external LSA. An Autonomous System Boundary Router (ASBR) can be configured to redistribute routes learned from other protocols by advertising an aggregate route into all attached autonomous systems. This helps both to decrease the number of external LSAs and the size of the OSPF link state database.

EXAMPLE

This example creates a summary address for all routes contained in 192.168.x.x.

```
Console(config-router)#summary-address 192.168.0.0 255.255.0.0  
Console(config-router)#
```

RELATED COMMANDS

[area range \(887\)](#)

[redistribute \(889\)](#)

Area Configuration

area nssa This command defines a not-so-stubby area (NSSA). To remove an NSSA, use the **no** form without any optional keywords. To remove an optional attribute, use the **no** form without the relevant keyword.

SYNTAX

```
[no] area area-id nssa
[translator-role [candidate | never | always]] |
[no-redistribution] | [no-summary] | [default-information-originate]
[metric metric-value | metric-type type-value]
```

area-id - Identifies the NSSA. The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.

translator-role - Indicates NSSA-ABR translator role for Type 5 external LSAs.

candidate - Router translates NSSA LSAs to Type-5 external LSAs if elected.

never - Router never translates NSSA LSAs to Type-5 external LSAs.

always - Router always translates NSSA LSAs to Type-5 external LSAs.

no-redistribution - Use this keyword when the router is an NSSA Area Border Router (ABR) and you want the **redistribute** command to import routes only into normal areas, and not into the NSSA. In other words, this keyword prevents the NSSA ABR from advertising external routing information (learned via routers in other areas) into the NSSA.

no-summary - Allows an area to retain standard NSSA features, but does not inject inter-area routes into this area.

default-information-originate - When the router is an NSSA Area Border Router (ABR) or an NSSA Autonomous System Boundary Router (ASBR), this parameter causes it to generate Type-7 default LSA into the NSSA. This default provides a route to other areas within the AS for an NSSA ABR, or to areas outside the AS for an NSSA ASBR.

metric-value - Metric assigned to Type-7 default LSAs.
(Range: 1-16777214; Default: 1)

type-value

1 - Type 1 external route

2 - Type 2 external route (default) - Routers do not add internal cost to the external route metric.

COMMAND MODE

Router Configuration

DEFAULT SETTING

No NSSA is configured.

COMMAND USAGE

- ◆ All routers in a NSSA must be configured with the same area ID.
- ◆ An NSSA is similar to a stub, because when the router is an ABR, it can send a default route for other areas in the AS into the NSSA using the **default-information-originate** keyword. However, an NSSA is different from a stub, because when the router is an ASBR, it can import a default external AS route (for routing protocol domains adjacent to the NSSA but not within the OSPF AS) into the NSSA using the **default-information-originate** keyword.
- ◆ External routes advertised into an NSSA can include network destinations outside the AS learned via OSPF, the default route, static routes, routes imported from other routing protocols such as RIP, and networks directly connected to the router that are not running OSPF.
- ◆ NSSA external LSAs (Type 7) are converted by any ABR adjacent to the NSSA into external LSAs (Type-5), and propagated into other areas within the AS.
- ◆ Also, note that unlike stub areas, all Type-3 summary LSAs are always imported into NSSAs to ensure that internal routes are always chosen over Type-7 NSSA external routes.
- ◆ This router supports up to 16 total areas (either normal transit areas, stubs, or NSSAs).

EXAMPLE

This example creates a stub area 10.3.0.0, and assigns all interfaces with class B addresses 10.3.x.x to the NSSA. It also instructs the router to generate external LSAs into the NSSA when it is an NSSA ABR or NSSA ASBR.

```
Console(config-router)#area 10.3.0.0 nssa default-information-originate
Console(config-router)#network 10.3.0.0 255.255.0.0 area 10.2.0.0
Console(config-router)#
```

area stub This command defines a stub area. To remove a stub, use the **no** form without the optional keyword. To remove the summary attribute, use the **no** form with the summary keyword.

SYNTAX

[no] area area-id stub [no-summary]

area-id - Identifies the stub area. The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.

no-summary - Stops an Area Border Router (ABR) from sending summary link advertisements into the stub area.

COMMAND MODE

Router Configuration

DEFAULT SETTING

No stub is configured.

Summary advertisement are sent into the stub.

COMMAND USAGE

- ◆ All routers in a stub must be configured with the same area ID.
- ◆ Routing table space is saved in a stub by blocking Type-4 AS summary LSAs and Type 5 external LSAs. The default setting for this command completely isolates the stub by blocking Type-3 summary LSAs that advertise the default route for destinations external to the local area or the autonomous system.
- ◆ Use the **no-summary** parameter of this command on the ABR attached to the stub to define a totally stubby area. Define an area as a totally stubby area only if routers in the area do not require summary LSAs from other areas.
- ◆ Use the [area default-cost](#) command to specify the cost of a default summary route sent into a stub by an ABR attached to the stub area.

EXAMPLE

This example creates a stub area 10.2.0.0, and assigns all interfaces with class B addresses 10.2.x.x to the stub.

```
Console(config-router)#area 10.2.0.0 stub
Console(config-router)#network 10.2.0.0 0.255.255.255 area 10.2.0.0
Console(config-router)#
```

RELATED COMMANDS

[area default-cost \(845\)](#)

area virtual-link This command defines a virtual link. To remove a virtual link, use the **no** form with no optional keywords. To restore the default value for an attribute, use the **no** form with the required keyword.

SYNTAX

```
area area-id virtual-link router-id  
    [authentication] [dead-interval seconds] [hello-interval seconds]  
    [retransmit-interval seconds] [transmit-delay seconds]  
  
no area area-id virtual-link router-id  
    [authentication | dead-interval | hello-interval | retransmit-interval |  
    transmit-delay]  
  
area area-id virtual-link router-id  
    authentication [message-digest | null]  
    [authentication-key key | message-digest-key key-id md5 key]  
  
no area area-id virtual-link router-id  
    authentication [authentication-key |  
    message-digest-key key-id]  
  
area area-id virtual-link router-id  
    [authentication-key key | message-digest-key key-id md5 key]  
  
no area area-id virtual-link router-id  
    [authentication-key | message-digest-key key-id]
```

area-id - Identifies the transit area for the virtual link. The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.

router-id - Router ID of the virtual link neighbor. This specifies the Area Border Router (ABR) at the other end of the virtual link. To create a virtual link, enter this command for an ABR at both ends of the link. One of the ABRs must be next to the isolated area and the transit area at one end of the link, while the other ABR must be next to the transit area and backbone at the other end of the link.

dead-interval *seconds* - Specifies the time that neighbor routers will wait for a hello packet before they declare the router down. This value must be the same for all routers attached to an autonomous system. (Range: 1-65535 seconds; Default: 4 x hello interval, or 40 seconds)

hello-interval *seconds* - Specifies the transmit delay between sending hello packets. Setting the hello interval to a smaller value can reduce the delay in detecting topological changes, but will increase the routing traffic. This value must be the same for all routers attached to an autonomous system. (Range: 1-65535 seconds; Default: 10 seconds)

retransmit-interval *seconds* - Specifies the interval at which the ABR retransmits link-state advertisements (LSA) over the virtual link. The retransmit interval should be set to a conservative value that provides an adequate flow of routing information, but does not produce unnecessary

protocol traffic. However, note that this value should be larger for virtual links. (Range: 1-3600 seconds; Default: 5 seconds)

transmit-delay *seconds* - Estimates the time required to send a link-state update packet over the virtual link, considering the transmission and propagation delays. LSAs have their age incremented by this amount before transmission. This value must be the same for all routers attached to an autonomous system. (Range: 1-65535 seconds; Default: 1 second)

authentication - Specifies the authentication mode. If no optional parameters follow this keyword, then plain text authentication is used along with the password specified by the **authentication-key**. If **message-digest** authentication is specified, then the **message-digest-key** and **md5** parameters must also be specified. If the **null** option is specified, then no authentication is performed on any OSPF routing protocol messages.

message-digest - Specifies message-digest (MD5) authentication.

null - Indicates that no authentication is used.

authentication-key *key* - Sets a plain text password (up to 8 characters) that is used by neighboring routers on a virtual link to generate or verify the authentication field in protocol message headers. A separate password can be assigned to each network interface. However, this key must be the same for all neighboring routers on the same network (i.e., autonomous system). This key is only used when authentication is enabled for the backbone.

message-digest-key *key-id* **md5** *key* - Sets the key identifier and password to be used to authenticate protocol messages passed between neighboring routers and this router when using message digest (MD5) authentication. The *key-id* is an integer from 0-255, and the *key* is an alphanumeric string up to 16 characters long. If MD5 authentication is used on a virtual link, then it must be enabled on all routers within an autonomous system; and the key identifier and key must also be the same for all routers.

COMMAND MODE

Router Configuration

DEFAULT SETTING

area-id: None

router-id: None

hello-interval: 10 seconds

retransmit-interval: 5 seconds

transmit-delay: 1 second

dead-interval: 40 seconds

authentication-key: None

message-digest-key: None

COMMAND USAGE

- ◆ All areas must be connected to a backbone area (0.0.0.0) to maintain routing connectivity throughout the autonomous system. If it not possible to physically connect an area to the backbone, you can use a virtual link. A virtual link can provide a logical path to the backbone for an isolated area, or can be configured as a backup connection that can take over if the normal connection to the backbone fails.
- ◆ A virtual link can be configured between any two backbone routers that have an interface to a common non-backbone area. The two routers joined by a virtual link are treated as if they were connected by an unnumbered point-to-point network.
- ◆ Any area disconnected from the backbone must include the transit area ID and the router ID for a virtual link neighbor that is adjacent to the backbone.

EXAMPLE

This example creates a virtual link using the defaults for all optional parameters.

```
Console(config-router)#network 10.4.0.0 0.255.255.0.0 area 10.4.0.0
Console(config-router)#area 10.4.0.0 virtual-link 10.4.3.254
Console(config-router)#
```

This example creates a virtual link using MD5 authentication.

```
Console(config-router)#network 10.4.0.0 0.255.255.0.0 area 10.4.0.0
Console(config-router)#area 10.4.0.0 virtual-link 10.4.3.254 message-digest-
key 5 md5 ld83jdpq
Console(config-router)#
```

RELATED COMMANDS

[show ip protocols ospf \(879\)](#)

network area This command defines an OSPF area and the interfaces that operate within this area. Use the **no** form to disable OSPF for a specified interface.

SYNTAX

[no] network *ip-address netmask area area-id*

ip-address - Address of the interfaces to add to the area.

netmask - Network mask of the address range to add to the area.

area-id - Area to which the specified address or range is assigned. An OSPF area identifies a group of routers that share common routing information. The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

- ◆ An area ID uniquely defines an OSPF broadcast area. The area ID 0.0.0.0 indicates the OSPF backbone for an autonomous system. Each router must be connected to the backbone via a direct connection or a virtual link.
- ◆ Set the area ID to the same value for all routers on a network segment using the network mask to add one or more interfaces to an area.
- ◆ If an address range is overlapped in subsequent network area commands, the router will use the network area with the address range that most closely matches the interface address. Also, note that if a more specific address range is removed from an area, the interface belonging to that range may still remain active if a less specific address range covering that area has been specified.

EXAMPLE

This example creates the backbone 0.0.0.0 covering class B addresses 10.1.x.x, and a normal transit area 10.2.9.0 covering the class C addresses 10.2.9.x.

```
Console(config-router)#network 10.1.0.0 255.255.0.0 area 0.0.0.0
Console(config-router)#network 10.2.9.0 255.255.255.0 area 10.1.0.0
Console(config-router)#
```

Interface Configuration

ip ospf authentication This command specifies the authentication type used for an interface. Enter this command without any optional parameters to specify plain text (or simple password) authentication. Use the **no** form to restore the default of no authentication.

SYNTAX

ip ospf [*ip-address*] **authentication** [**message-digest** | **null**]

no ip ospf [*ip-address*] **authentication**

ip-address - IP address of the interface. Enter this parameter to specify a unique authentication type for a primary or secondary IP address associated with the current VLAN. If not specified, the command applies to all networks connected to the current interface.

message-digest - Specifies message-digest (MD5) authentication.

null - Indicates that no authentication is used.

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

No authentication

COMMAND USAGE

- ◆ Use authentication to prevent routers from inadvertently joining an unauthorized area. Configure routers in the same area with the same password or key. All neighboring routers on the same network with the same password will exchange routing data.
- ◆ This command creates a password (key) that is inserted into the OSPF header when routing protocol packets are originated by this device. Assign a separate password to each network for different interfaces.
- ◆ When using simple password authentication, a password is included in the packet. If it does not match the password configured on the receiving router, the packet is discarded. This method provides very little security as it is possible to learn the authentication key by snooping on routing protocol packets.
- ◆ When using Message-Digest 5 (MD5) authentication, the router uses the MD5 algorithm to verify data integrity by creating a 128-bit message digest from the authentication key. Without the proper key and key-id, it is nearly impossible to produce any message that matches the pre-specified target message digest.
- ◆ Before specifying plain-text password authentication for an interface, configure a password with the [ip ospf authentication-key](#) command. Before specifying MD5 authentication for an interface, configure the message-digest key-id and key with the [ip ospf message-digest-key](#) command.
- ◆ The plain-text authentication-key, or the MD5 *key-id* and *key*, must be used consistently throughout the autonomous system.

EXAMPLE

This example enables message-digest authentication for the specified interface.

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf authentication message-digest
Console(config-if)#
```

RELATED COMMANDS

[ip ospf authentication-key \(859\)](#)

[ip ospf message-digest-key \(862\)](#)

ip ospf authentication-key This command assigns a simple password to be used by neighboring routers to verify the authenticity of routing protocol messages. Use the **no** form to remove the password.

SYNTAX

ip ospf [*ip-address*] **authentication-key** *key*

no ip ospf [*ip-address*] **authentication-key**

ip-address - This parameter can be used to indicate a specific IP address connected to the current interface. If not specified, the command applies to all networks connected to the current interface.

key - Sets a plain text password. (Range: 1-8 characters)

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

No password

COMMAND USAGE

- ◆ Before specifying plain-text password authentication for an interface with the [ip ospf authentication](#) command, configure a password with this command.
- ◆ This command creates a password (key) that is inserted into the OSPF header when routing protocol packets are originated by this device. Assign a separate password to each network for different interfaces. All neighboring routers on the same network with the same password will exchange routing data.
- ◆ A different password can be assigned to each network interface, but the password must be used consistently on all neighboring routers throughout a network (i.e., autonomous system).

EXAMPLE

This example sets a password for the specified interface.

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf authentication-key badboy
Console(config-if)#
```

RELATED COMMANDS

[ip ospf authentication \(857\)](#)

ip ospf cost This command explicitly sets the cost of sending a protocol packet on an interface, where higher values indicate slower ports. Use the **no** form to restore the default value.

SYNTAX

ip ospf [*ip-address*] **cost** *cost*

no ip ospf [*ip-address*] **cost**

ip-address - This parameter can be used to indicate a specific IP address connected to the current interface. If not specified, the command applies to all networks connected to the current interface.

cost - Link metric for this interface. Use higher values to indicate slower ports. (Range: 1-65535)

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

1

COMMAND USAGE

- ◆ The interface cost indicates the overhead required to send packets across a certain interface. This is advertised as the link cost in router link state advertisements.
- ◆ Routes are assigned a metric equal to the sum of all metrics for each interface link in the route.
- ◆ This router uses a default cost of 1 for all port types. Therefore, if any VLAN contains 10 Gbps ports, you may want to reset the cost for other VLANs which do not contain 10 Gbps ports to a value greater than 1.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf cost 10
Console(config-if)#
```

ip ospf dead-interval This command sets the interval at which hello packets are not seen before neighbors declare the router down. Use the **no** form to restore the default value.

SYNTAX

ip ospf [*ip-address*] **dead-interval** *seconds*

no ip ospf [*ip-address*] **dead-interval**

ip-address - This parameter can be used to indicate a specific IP address connected to the current interface. If not specified, the command applies to all networks connected to the current interface.

seconds - The maximum time that neighbor routers can wait for a hello packet before declaring the transmitting router down. This interval must be set to the same value for all routers on the network. (Range: 1-65535)

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

40, or four times the interval specified by the [ip ospf hello-interval](#) command.

COMMAND USAGE

The dead-interval is advertised in the router's hello packets. It must be a multiple of the hello-interval and be the same for all routers on a specific network.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf dead-interval 50
Console(config-if)#
```

RELATED COMMANDS

[ip ospf hello-interval \(861\)](#)

ip ospf hello-interval This command specifies the interval between sending hello packets on an interface. Use the **no** form to restore the default value.

SYNTAX

ip ospf [*ip-address*] **hello-interval** *seconds*

no ip ospf [*ip-address*] **hello-interval**

ip-address - This parameter can be used to indicate a specific IP address connected to the current interface. If not specified, the command applies to all networks connected to the current interface.

seconds - Interval at which hello packets are sent from an interface. This interval must be set to the same value for all routers on the network. (Range: 1-65535)

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

10 seconds

COMMAND USAGE

Hello packets are used to inform other routers that the sending router is still active. Setting the hello interval to a smaller value can reduce the delay in detecting topological changes, but will increase routing traffic.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf hello-interval 5
Console(config-if)#
```

ip ospf message-digest-key

This command enables message-digest (MD5) authentication on the specified interface and to assign a key-id and key to be used by neighboring routers. Use the **no** form to remove an existing key.

SYNTAX

ip ospf [*ip-address*] **message-digest-key** *key-id* **md5** *key*

no ip ospf [*ip-address*] **message-digest-key** *key-id*

ip-address - This parameter can be used to indicate a specific IP address connected to the current interface. If not specified, the command applies to all networks connected to the current interface.

key-id - Index number of an MD5 key. (Range: 0-255)

key - Alphanumeric password used to generate a 128 bit message digest or "fingerprint." (Range: 1-16 characters)

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

MD5 authentication is disabled.

COMMAND USAGE

- ◆ Before specifying MD5 authentication for an interface with the **ip ospf authentication** command, configure the message-digest key-id and key with this command.
- ◆ Normally, only one key is used per interface to generate authentication information for outbound packets and to authenticate incoming packets. Neighbor routers must use the same key identifier and key value.

- ◆ When changing to a new key, the router will send multiple copies of all protocol messages, one with the old key and another with the new key. Once all the neighboring routers start sending protocol messages back to this router with the new key, the router will stop using the old key. This rollover process gives the network administrator time to update all the routers on the network without affecting the network connectivity. Once all the network routers have been updated with the new key, the old key should be removed for security reasons.

EXAMPLE

This example sets a message-digest key identifier and password.

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf message-digest-key 1 md5 aiebel
Console(config-if)#
```

RELATED COMMANDS

[ip ospf authentication \(857\)](#)

ip ospf priority This command sets the router priority used when determining the designated router (DR) and backup designated router (BDR) for an area. Use the **no** form to restore the default value.

SYNTAX

ip ospf [*ip-address*] **priority** *priority*

no ip ospf [*ip-address*] **priority**

ip-address - This parameter can be used to indicate a specific IP address connected to the current interface. If not specified, the command applies to all networks connected to the current interface.

priority - Sets the interface priority for this router. (Range: 0-255)

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

1

COMMAND USAGE

- ◆ A designated router (DR) and backup designated router (BDR) are elected for each OSPF network segment based on Router Priority. The DR forms an active adjacency to all other routers in the network segment to exchange routing topology information. If for any reason the DR fails, the BDR takes over this role.
- ◆ Set the priority to zero to prevent a router from being elected as a DR or BDR. If set to any value other than zero, the router with the highest priority will

become the DR and the router with the next highest priority becomes the BDR. If two or more routers are tied with the same highest priority, the router with the higher ID will be elected.

- ◆ If a DR already exists for a network segment when this interface comes up, the new router will accept the current DR regardless of its own priority. The DR will not change until the next time the election process is initiated.
- ◆ Configure router priority for multi-access networks only and not for point-to-point networks.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf priority 5
Console(config-if)#
```

ip ospf retransmit-interval This command specifies the time between resending link-state advertisements (LSAs). Use the **no** form to restore the default value.

SYNTAX

ip ospf [*ip-address*] **retransmit-interval** *seconds*

no ip ospf [*ip-address*] **retransmit-interval**

ip-address - This parameter can be used to indicate a specific IP address connected to the current interface. If not specified, the command applies to all networks connected to the current interface.

seconds - Sets the interval at which LSAs are retransmitted from this interface. (Range: 1-65535)

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

5 seconds

COMMAND USAGE

- ◆ A router will resend an LSA to a neighbor if it receives no acknowledgment after the specified retransmit interval. The retransmit interval should be set to a conservative value that provides an adequate flow of routing information, but does not produce unnecessary protocol traffic. Note that this value should be larger for virtual links.
- ◆ Set this interval to a value that is greater than the round-trip delay between any two routers on the attached network to avoid unnecessary retransmissions.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf retransmit-interval 7
Console(config-if)#
```

ip ospf transmit-delay This command sets the estimated time to send a link-state update packet over an interface. Use the **no** form to restore the default value.

SYNTAX

ip ospf [*ip-address*] **transmit-delay** *seconds*

no ip ospf [*ip-address*] **transmit-delay**

ip-address - This parameter can be used to indicate a specific IP address connected to the current interface. If not specified, the command applies to all networks connected to the current interface.

seconds - Sets the estimated time required to send a link-state update.
(Range: 1-65535)

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

1 second

COMMAND USAGE

- ◆ LSAs have their age incremented by this delay before transmission. When estimating the transmit delay, consider both the transmission and propagation delays for an interface. Set the transmit delay according to link speed, using larger values for lower-speed links.
- ◆ If this delay is not added, the time required to transmit an LSA over the link is not taken into consideration by the routing process. On slow links, the router may send packets more quickly than devices can receive them. To avoid this problem, use the transmit delay to force the router to wait a specified interval between transmissions.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf transmit-delay 6
Console(config-if)#
```

passive-interface This command suppresses OSPF routing traffic on the specified interface. Use the **no** form to allow routing traffic to be sent and received on the specified interface.

SYNTAX

[no] passive-interface vlan *vlan-id* [*ip-address*]

vlan-id - VLAN ID. (Range: 1-4094)

ip-address - An IPv4 address configured on this interface.

COMMAND MODE

Router Configuration

DEFAULT SETTING

None

COMMAND USAGE

You can configure an OSPF interface as passive to prevent OSPF routing traffic from exiting or entering that interface. No OSPF adjacency can be formed if one of the interfaces involved is set to passive mode. The specified interface will appear as a stub in the OSPF domain. Also, if you configure an OSPF interface as passive where an adjacency already exists, the adjacency will drop almost immediately.

EXAMPLE

```
Console(config-router)#passive-interface vlan 1
Console(config-router)#
```

Display Information

show ip ospf This command shows basic information about the routing configuration.

SYNTAX

show ip ospf [*process-id*]

process-id - The ID of the router process for which information will be displayed. (Range: 1-65535)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip ospf
Routing Process "ospf 1" with ID 192.168.1.3
Process uptime is 20 minutes
Conforms to RFC2328, and RFC1583Compatibility flag is disabled
Supports only single TOS(TOS0) routes
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Refresh timer 10 secs
Number of incoming current DD exchange neighbors 0/5
```

```

Number of outgoing current DD exchange neighbors 0/5
Number of external LSA 0. Checksum 0x000000
Number of opaque AS LSA 0. Checksum 0x000000
LSDB database overflow limit is 20480
Number of LSA originated 1
Number of LSA received 0
Number of areas attached to this router: 1

Area 192.168.1.3
  Number of interfaces in this area is 1(1)
  Number of fully adjacent neighbors in this area is 0
  Area has no authentication
  SPF algorithm last executed 00:00:08.739 ago
  SPF algorithm executed 1 times
  Number of LSA 1. Checksum 0x007f09
Console#

```

Table 179: show ip ospf - display description

Field	Description
Routing Process with ID	OSPF process ID and router ID. The router ID uniquely identifies the router in the autonomous system. By convention, this is normally set to one of the router's IP interface addresses.
Process uptime	The time this process has been running
Conforms to RFC2328	Shows that this router is compliant with OSPF Version 2.
RFC1583 Compatibility flag	Shows whether or not compatibility with the RFC 1583 (an earlier version of OSPFv2) is enabled.
Supports only single TOS (TOS0) routes	Optional Type of Service (ToS) specified in OSPF Version 2, Appendix F.1.2 is not supported, so only one cost per interface can be assigned.
SPF schedule delay	Delay between receiving a change to SPF calculation.
Hold time	Sets the hold time between two consecutive SPF calculations.
Refresh timer	The time between refreshing the LSA database.
Number of current DD exchange neighbors	Number of neighbors currently exchanging database descriptor packets.
Number of external LSA	The number of external link-state advertisements (Type 5 LSAs) in the link-state database. These LSAs advertise information about routes outside of the autonomous system.
Checksum	The sum of the LS checksums of the external link-state advertisements contained in the link-state database.
Number of opaque AS LSA	Number of opaque link-state advertisements (Type 9, 10 and 11 LSAs) in the link-state database. These LSAs advertise information about external applications, and are only used by OSPF for the graceful restart process.
Checksum	The sum of the LS checksums of opaque link-state advertisements contained in the link-state database.
LSDB database overflow limit	The maximum number of LSAs allowed in the external database.
Number of LSA originated	The number of new link-state advertisements that have been originated.
Number of LSA received	The number of link-state advertisements that have been received.

Table 179: show ip ospf - display description (Continued)

Field	Description
Number of areas attached to this router	The number of configured areas attached to this router.
Number of interfaces in this area is	The number of interfaces attached to this area
Number of fully adjacent neighbors in this area is	The number of neighbors for which the exchange of recognition protocol messages has been completed and are now fully adjacent
Area has (no) authentication	Shows whether or not the authentication has been enabled
SPF algorithm last executed	The last time the shortest path first algorithm was executed
SPF algorithm executed x times	The number of times the shortest path first algorithm has been executed for this area
Number of LSA	The number of new link-state advertisements that have been originated.
Checksum	The sum of the link-state advertisements' LS checksums contained in this area's link-state database.

show ip ospf border-routers This command shows entries in the routing table that lead to an Area Border Router (ABR) or Autonomous System Boundary Router (ASBR).

SYNTAX

show ip ospf [process-id] border-routers

process-id - The ID of the router process for which information will be displayed. (Range: 1-65535)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip ospf border-routers

OSPF process 1 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 192.168.0.3 [1] via 192.168.0.3, vlan1, ABR, ASBR, Area 0.0.0.0
Console#
```

show ip ospf database This command shows information about different OSPF Link State Advertisements (LSAs) stored in this router's database.

SYNTAX

show ip ospf [*process-id*] **database**
 [**asbr-summary** | **external** | **network** | **nssa-external** | **router** | **summary**]
 [**adv-router** *ip-address* | *link-state-id* | **self-originate**]

process-id - The ID of the router process for which information will be displayed. (Range: 1-65535)

adv-router - IP address of the advertising router. If not entered, information about all advertising routers is displayed.

ip-address - IP address of the specified router. If no address is entered, information about the local router is displayed.

link-state-id - The network portion described by an LSA. The *link-state-id* entered should be:

- An IP network number for Type 3 Summary and External LSAs
- A Router ID for Router, Network, and Type 4 AS Summary LSAs

Also, note that when an Type 5 ASBR External LSA is describing a default route, its *link-state-id* is set to the default destination (0.0.0.0).

self-originate - Shows LSAs originated by this router.

asbr-summary - Shows information about Autonomous System Boundary Router summary LSAs.

external - Shows information about external LSAs.

network - Shows information about network LSAs.

nssa-external - Shows information about NSSA external LSAs.

router - Shows information about router LSAs.

summary - Shows information about summary LSAs.

COMMAND MODE

Privileged Exec

EXAMPLES

The following shows output for the **show ip ospf database** command.

```
Console#show ip ospf database
```

```
OSPF Router with ID (192.168.0.2) (Process ID 1)
```

```
Router Link States (Area 0.0.0.0)
```

Link ID	ADV Router	Age	Seq#	CkSum	Link count
192.168.0.2	192.168.0.2	225	0x80000004	0xdac5	1
192.168.0.3	192.168.0.3	220	0x80000004	0xd8c4	1

```

Net Link States (Area 0.0.0.0)

Link ID        ADV Router    Age  Seq#           CkSum
192.168.0.2    192.168.0.2    225  0x80000001    0x9c0f

AS External Link States

Link ID        ADV Router    Age  Seq#           CkSum  Route          Tag
0.0.0.0        192.168.0.2    487  0x80000001    0xd491  E2 0.0.0.0/0  0
0.0.0.0        192.168.0.3    222  0x80000001    0xce96  E2 0.0.0.0/0  0

Console#

```

Table 180: show ip ospf database - display description

Field	Description
OSPF Router Process with ID	OSPF process ID and router ID. The router ID uniquely identifies the router in the autonomous system. By convention, this is normally set to one of the router's IP interface addresses.
Link ID	Either a Router ID or an IP Address; it identifies the piece of the routing domain that is being described by the advertisement
ADV Router	Advertising router ID
Age	Age of LSA (in seconds)
Seq#	Sequence number of LSA (used to detect older duplicate LSAs)
CkSum	Checksum of the complete contents of the LSA
Link count	Number of interfaces attached to the router
Route	Type 1 or Type 2 external metric (see the redistribute command) and route
Tag	Optional tag if defined (see the redistribute command)

The following shows output when using the **asbr-summary** keyword.

```

Console#show ip ospf database asbr-summary

OSPF Router with ID (0.0.0.0) (Process ID 1)

ASBR-Summary Link States (Area 0.0.0.1)

LS Age: 0
Options: 0x2 (*|-|-|-|-|E|-)
LS Type: ASBR-summary-LSA
Link State ID: 2.1.0.0 (AS Boundary Router address)
Advertising Router: 192.168.2.1
LS Seq Number: 80000001
Checksum: 0x7b67
Length: 28
Network Mask: /0
TOS: 0 Metric: 10

Console#

```

Table 181: show ip ospf database summary - display description

Field	Description
OSPF Router ID	Router ID
LS Age	Age of LSA (in seconds)
Options	Optional capabilities associated with the LSA
LS Type	Summary Links - LSA describes routes to AS boundary routers
Link State ID	Interface address of the autonomous system boundary router
Advertising Router	Advertising router ID
LS Sequence Number	Sequence number of LSA (used to detect older duplicate LSAs)
Checksum	Checksum of the complete contents of the LSA
Length	The length of the LSA in bytes
Network Mask	Address mask for the network
TOS	Type of Service – This router only supports TOS 0 (or normal service)
Metric	Cost of the link

The following shows output when using the **external** keyword.

```

Console#show ip ospf database external
OSPF Router process 100 with ID (10.10.11.50)
AS External Link States LS age: 298
Options: 0x2 (*|-|-|-|-|E|-)
LS Type: AS-external-LSA
Link State ID: 10.10.100.0 (External Network Number)
Advertising Router: 10.10.11.50
LS Seq Number: 80000001
Checksum: 0x7033
Length: 36
Network Mask: /24
Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 20
Forward Address: 10.10.11.50
External Route Tag: 0

OSPF Router with ID (0.0.0.0) (Process ID 1)

AS External Link States

LS Age: 0
Options: 0x2 (*|-|-|-|-|E|-)
LS Type: AS-external-LSA
Link State ID: 0.0.0.0 (External Network Number)
Advertising Router: 192.168.0.2
LS Seq Number: 80000005
Checksum: 0xcc95
Length: 36
Network Mask: /0
Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 1

```

```
Forward Address: 0.0.0.0
External Route Tag: 0
```

```
Console#
```

Table 182: show ip ospf database external - display description

Field	Description
OSPF Router ID	Router ID
LS Age	Age of LSA (in seconds)
Options	Optional capabilities associated with the LSA
LS Type	AS External Links - LSA describes routes to destinations outside the AS (including default external routes for the AS)
Link State ID	IP network number (External Network Number)
Advertising Router	Advertising router ID
LS Sequence Number	Sequence number of LSA (used to detect older duplicate LSAs)
Checksum	Checksum of the complete contents of the LSA
Length	The length of the LSA in bytes
Network Mask	Address mask for the network
Metric Type	Type 1 or Type 2 external metric (see the redistribute command)
TOS	Type of Service – This router only supports TOS 0 (or normal service)
Metric	Cost of the link
Forward Address	Next hop address. If this field is set to 0.0.0.0, data is forwarded to the originator of the advertisement.
External Route Tag	Optional tag if defined (see the redistribute command)

The following shows output when using the **network** keyword.

```
Console#show ip ospf database network

OSPF Router with ID (0.0.0.0) (Process ID 1)

Net Link States (Area 0.0.0.0)

LS Age: 0
Options: 0x2 (*|-|-|-|-|E|-)
LS Type: network-LSA
Link State ID: 192.168.0.2 (address of Designated Router)
Advertising Router: 192.168.0.2
LS Seq Number: 80000005
Checksum: 0x9413
Length: 32
Network Mask: /24
    Attached Router: 192.168.0.2
    Attached Router: 192.168.0.3
.
```


:

Table 183: show ip ospf database network - display description

Field	Description
OSPF Router ID	Router ID
LS Age	Age of LSA (in seconds)
Options	Optional capabilities associated with the LSA
LS Type	Network Link - LSA describes the routers attached to the network
Link State ID	Interface address of the designated router
Advertising Router	Advertising router ID
LS Sequence Number	Sequence number of LSA (used to detect older duplicate LSAs)
Checksum	Checksum of the complete contents of the LSA
Length	The length of the LSA in bytes
Network Mask	Address mask for the network
Attached Router	List of routers attached to the network; i.e., fully adjacent to the designated router, including the designated router itself

The following shows output when using the **router** keyword.

```

Console#show ip ospf database router

      OSPF Router with ID (0.0.0.0) (Process ID 1)

      Router Link States (Area 0.0.0.0)

LS Age: 0
Options: 0x2 (*|-|-|-|-|E|-)
Flags: 0x2 : ASBR
LS Type: router-LSA
Link State ID: 192.168.0.2
Advertising Router: 192.168.0.2
LS Seq Number: 80000008
Checksum: 0xd2c9
Length: 36
  Link connected to: a Transit Network
    (Link ID) Designated Router address: 192.168.0.2
    (Link Data) Router Interface address: 192.168.0.2
    Number of TOS metrics: 0
    TOS 0 Metric: 1
:
:
:

```

Table 184: show ip ospf database router - display description

Field	Description
OSPF Router ID	Router ID
LS Age	Age of LSA (in seconds)
Options	Optional capabilities associated with the LSA
Flags	Indicate if this router is a virtual link endpoint, an ASBR, or an ABR
LS Type	Router Link - LSA describes the router's interfaces.
Link State ID	Router ID of the router that originated the LSA
Advertising Router	Advertising router ID
LS Sequence Number	Sequence number of LSA (used to detect older duplicate LSAs)
Checksum	Checksum of the complete contents of the LSA
Length	The length of the LSA in bytes
Link connected to	Link-state type, including transit network, stub network, or virtual link
Link ID	Link type and corresponding Router ID or network address
Link Data	<ul style="list-style-type: none"> ♦ Router ID for transit network ♦ Network's IP address mask for stub network ♦ Neighbor Router ID for virtual link
Number of TOS metrics	Type of Service metric – This router only supports TOS 0 (or normal service)
TOS	Type of Service – This router only supports TOS 0 (or normal service)
Metric	Cost of the link

The following shows output when using the **summary** keyword.

```

Console#show ip ospf database summary

      OSPF Router with ID (0.0.0.0) (Process ID 1)

      Summary Link States (Area 0.0.0.0)

LS Age: 1
Options: 0x0 (*|-|-|-|-|-|-)
LS Type: summary-LSA
Link State ID: 192.168.10.0 (summary Network Number)
Advertising Router: 2.1.0.0
LS Seq Number: 80000005
Checksum: 0x479d
Length: 28
Network Mask: /24
      TOS: 0  Metric: 0
:

```

Table 185: show ip ospf database summary - display description

Field	Description
OSPF Router ID	Router ID
LS Age	Age of LSA (in seconds)
Options	Optional capabilities associated with the LSA
LS Type	Summary Links - LSA describes routes to networks
Link State ID	Router ID of the router that originated the LSA
Advertising Router	Advertising router ID
LS Sequence Number	Sequence number of LSA (used to detect older duplicate LSAs)
Checksum	Checksum of the complete contents of the LSA
Length	The length of the LSA in bytes
Network Mask	Destination network's IP address mask
Metrics	Cost of the link

show ip ospf interface This command displays summary information for OSPF interfaces.

SYNTAX

show ip ospf interface [vlan *vlan-id*]

vlan-id - VLAN ID (Range: 1-4094)

COMMAND MODE

Privileged Exec

EXAMPLE

```

Console#show ip ospf interface vlan 1
VLAN1 is up, line protocol is up
  Internet Address 192.168.0.2/24, Area 0.0.0.0, MTU 1500
  Process ID 1, Router ID 192.168.0.2, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.0.2, Interface Address 192.168.0.2
  Backup Designated Router (ID) 192.168.0.3, Interface Address 192.168.0.3
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:10
  Neighbor Count is 1, Adjacent neighbor count is 1
  Hello received 920 sent 975, DD received 5 sent 4
  LS-Req received 1 sent 1, LS-Upd received 14 sent 18
  LS-Ack received 17 sent 13, Discarded 0
Console#

```

Table 186: show ip ospf interface - display description

Field	Description
VLAN	VLAN ID and Status of physical link
Internet Address	IP address of OSPF interface
Area	OSPF area to which this interface belongs
MTU	Maximum transfer unit
Process ID	OSPF process ID
Router ID	Router ID
Network Type	Includes broadcast, non-broadcast, or point-to-point networks
Cost	Interface transmit cost
Transmit Delay	Interface transmit delay (in seconds)
State	<ul style="list-style-type: none"> ◆ Disabled – OSPF not enabled on this interface ◆ Down – OSPF is enabled on this interface, but interface is down ◆ Loopback – This is a loopback interface ◆ Waiting – Router is trying to find the DR and BDR ◆ DR – Designated Router ◆ BDR – Backup Designated Router ◆ DRother – Interface is on a multiaccess network, but is not the DR or BDR
Priority	Router priority
Designated Router	Designated router ID and respective interface address
Backup Designated Router	Backup designated router ID and respective interface address
Timer intervals	Configuration settings for timer intervals, including Hello, Dead and Retransmit
Neighbor Count	Count of network neighbors and adjacent neighbors
Adjacent neighbor count	Count of adjacent neighbors
Hello	Number of Hello LSAs received and sent
DD	Number of Database Descriptor packets received and sent.
LS-Req	Number of LSA requests
LS-Upd	Number of LSA updates
LS-Ack	Number of LSA acknowledgements
Discarded	Number of LSAs discarded

show ip ospf neighbor This command displays information about neighboring routers on each interface within an OSPF area.

SYNTAX

show ip ospf [*process-id*] **neighbor**

process-id - The ID of the router process for which information will be displayed. (Range: 1-65535)

COMMAND MODE

Privileged Exec

EXAMPLE

```

Console#show ip ospf neighbor

```

ID	Pri	State	Address	Interface
192.168.0.3	1	FULL/BDR	192.168.0.3	VLAN1

```

Console#

```

Table 187: show ip ospf neighbor - display description

Field	Description
Neighbor ID	Neighbor's router ID
Pri	Neighbor's router priority
State	OSPF state and identification flag States include: Down – Connection down Attempt – Connection down, but attempting contact (for non-broadcast networks) Init – Have received Hello packet, but communications not yet established Two-way – Bidirectional communications established ExStart – Initializing adjacency between neighbors Exchange – Database descriptions being exchanged Loading – LSA databases being exchanged Full – Neighboring routers now fully adjacent Identification flags include: D – Dynamic neighbor S – Static neighbor DR – Designated router BDR – Backup designated router
Address	IP address of this interface
Interface	The interface to which this neighbor is attached

show ip ospf route This command displays the OSPF routing table.

SYNTAX

show ip ospf [*process-id*] **route**

process-id - The ID of the router process for which information will be displayed. (Range: 1-65535)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip ospf route
OSPF process 1:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
O  10.10.0.0/24 [10] is directly connected, fe1/1, Area 0.0.0.0
O  10.10.11.0/24 [10] is directly connected, fe1/2, Area 0.0.0.0
O  10.10.11.100/32 [10] is directly connected, lo, Area 0.0.0.0
E2 10.15.0.0/24 [10/50] via 10.10.0.1, VLAN1
IA 172.16.10.0/24 [30] via 10.10.11.50, VLAN2, Area 0.0.0.0
E2 192.168.0.0/16 [10/20] via 10.10.11.50, VLAN2
```

```
Console#
```

show ip ospf virtual-links This command displays detailed information about virtual links.

SYNTAX

show ip ospf virtual-links

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip ospf virtual-links
Virtual Link VLINK1 to router 192.168.0.2 is up
Transit area 0.0.0.1 via interface VLAN1
Local address 192.168.0.3
Remote address 192.168.0.2
Transmit Delay is 1 sec, State Point-To-Point,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:08
Adjacency state Down
Console#
```

Table 188: show ip ospf virtual-links - display description

Field	Description
Virtual Link to router	OSPF neighbor and link state (up or down)
Transit area	Common area the virtual link crosses to reach the target router
Local address	The IP address of ABR that serves as an endpoint connecting the isolated area to the common transit area.
Remote address	The IP address this virtual neighbor is using. The neighbor must be an ABR at the other endpoint connecting the common transit area to the backbone itself.
Transmit Delay	Estimated transmit delay (in seconds) on the virtual link
Timer intervals	Configuration settings for timer intervals, including Hello, Dead and Retransmit

RELATED COMMANDS

[area virtual-link \(854\)](#)

show ip protocols ospf This command displays OSPF process parameters.

SYNTAX

show ip protocols ospf

COMMAND MODE

Privileged Exec

EXAMPLE

```

Console#show ip protocols ospf
Routing Protocol is "ospf 200"
Redistributing: rip
Routing for Networks:
  192.30.30.0/24
  192.40.40.0/24
  Routing for Summary Address:
    192.168.1.0/24
    192.168.3.0/24
Distance: (default is 110)
Console#

```

Table 189: show ip protocols ospf - display description

Field	Description
Routing Protocol	Name and autonomous system number of this OSPF process.
Redistributing	Shows if route redistribution has been enabled with the redistribute command.
Routing for Networks	Networks for which the OSPF is currently registering routing information.

Table 189: show ip protocols ospf - display description (Continued)

Field	Description
Routing for Summary Address	Shows the networks for which route summarization is in effect
Distance	The administrative distance used for external routes learned by OSPF (see the ip route command).

OPEN SHORTEST PATH FIRST (OSPFv3)

Table 190: Open Shortest Path First Commands (Version 3)

Command	Function	Mode
<i>General Configuration</i>		
router ipv6 ospf	Enables or disables OSPFv3 routing process	GC
abr-type	Sets the criteria used to determine if this router can declare itself an ABR and issue Type 3 and Type 4 summary LSAs	RC
max-current-dd	Sets the maximum number of neighbors with which the switch can concurrently exchange database descriptor packets	RC
router-id	Sets the router ID for this device	RC
timers spf	Configures the delay after a topology change and the hold time between consecutive SPF calculations	RC
<i>Route Metrics and Summaries</i>		
area default-cost	Sets the cost for a default summary route sent into a stub	RC
area range	Summarizes routes advertised by an ABR	RC
default-metric	Sets the default metric for external routes imported from other protocols	RC
redistribute	Redistribute routes from one routing domain to another	RC
<i>Area Configuration</i>		
area stub	Defines a stubby area that cannot send or receive LSAs	RC
area virtual-link	Defines a virtual link from an area border routers to the backbone	RC
ipv6 router ospf area	Binds an area to the selected interface	IC
ipv6 router ospf tag area	Binds an area to the selected interface and process	IC
<i>Interface Configuration</i>		
ipv6 ospf cost	Specifies the cost of sending a packet on an interface	IC
ipv6 ospf dead-interval	Sets the interval at which hello packets are not seen before neighbors declare the router down	IC
ipv6 ospf hello-interval	Specifies the interval between sending hello packets	IC
ipv6 ospf priority	Sets the router priority used to determine the designated router	IC

Table 190: Open Shortest Path First Commands (Version 3) (Continued)

Command	Function	Mode
<code>ipv6 ospf retransmit-interval</code>	Specifies the time between resending a link-state advertisement	IC
<code>ipv6 ospf transmit-delay</code>	Estimates time to send a link-state update packet over an interface	IC
<code>passive-interface</code>	Suppresses OSPF routing traffic on the specified interface	RC
<i>Display Information</i>		
<code>show ipv6 ospf</code>	Displays general information about the routing processes	PE
<code>show ipv6 ospf database</code>	Shows information about different LSAs in the database	PE
<code>show ipv6 ospf interface</code>	Displays interface information	PE
<code>show ipv6 ospf neighbor</code>	Displays neighbor information	PE
<code>show ipv6 ospf route</code>	Displays the OSPF routing table	PE
<code>show ipv6 ospf virtual-links</code>	Displays parameters and the adjacency state of virtual links	PE

General Guidelines

Follow these basic steps to configure OSPFv3:

1. Assign an IPv6 link-local address to each VLAN interface that will participate in an OSPF routing process. You can automatically generate a link-local address using the `ipv6 enable` command, or manually assign an address to an interface using the `ipv6 address link-local` command.
2. Use the `router ipv6 ospf` command to create a local OSPF router process and enter router configuration mode.
3. Use the `router-id` command to assign a unique identifier to the router. Note that the default router ID of “0.0.0.0” cannot be used with the current software version.
4. Use the `ipv6 router ospf area` command or the `ipv6 router ospf tag area` command to assign an area to each interface that will participate in the specified OSPF process.

General Configuration

router ipv6 ospf This command creates an Open Shortest Path First (OSPFv3) routing process and enters router configuration mode. Use the **no** form to disable OSPF for all processes or for a specified process.

SYNTAX

[no] router ipv6 ospf [tag process-name]

process-name - A process name must be entered when configuring multiple routing instances. (Range: Alphanumeric string up to 16 characters)

COMMAND MODE

Global Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

- ◆ This command is used to enable an OSPFv3 routing process, and to enter router configuration mode.
- ◆ The *process-name* is only used on the local router to distinguish between different routing processes. It should not be confused with the *instance-id* configured with the **ipv6 router ospf area** command which is used to distinguish between different routing processes running on the same link-local network segment.

EXAMPLE

```
Console(config)#router ipv6 ospf tag 0
Console(config-router)#end
Console#show ipv6 ospf
Routing Process "ospf r&d" with ID 192.168.0.2
Process uptime is 1 hour 34 minutes
Supports only single TOS(TOS0) routes
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Number of incoming concurrent DD exchange neighbors 0/5
Number of outgoing concurrent DD exchange neighbors 0/5
Number of external LSA 0. Checksum 0x000000
Number of opaque AS LSA 0. Checksum 0x000000
Number of LSA received 0
Number of areas attached to this router: 1

      Area 0.0.0.0 (BACKBONE)
        SPF algorithm executed 1 times
        Number of LSA 2. Checksum 0x00ab4f

Console#
```

RELATED COMMANDS

[ipv6 router ospf area \(893\)](#)

abr-type This command sets the criteria used to determine if this router can declare itself an ABR and issue Type 3 and Type 4 summary LSAs. Use the **no** form to restore the default setting.

SYNTAX

abr-type {**cisco** | **ibm** | **standard**}

no abr-type

cisco - ABR criteria and functional behavior is based on RFC 3509.

ibm - ABR criteria and functional behavior is briefly described in RFC 3509, and fully documented in IBM Nways Multiprotocol Routing Services (MRS) 3.3.

standard - ABR criteria and functional behavior is based on RFC 2328.

COMMAND MODE

Router Configuration

DEFAULT SETTING

cisco

COMMAND USAGE

- ◆ The basic criteria for a router to serve as an ABR is shown below:
 - Cisco Systems Interpretation: A router is considered to be an ABR if it has more than one area actively attached and one of them is the backbone area.
 - IBM Interpretation: A router is considered to be an ABR if it has more than one actively attached area and the backbone area is configured.
 - Standard Interpretation: A router is considered to be an ABR if it is attached to two or more areas. It does not have to be attached to the backbone area.
- ◆ To successfully route traffic to inter-area and AS external destinations, an ABR must be connected to the backbone. If an ABR has no backbone connection, all traffic destined for areas not connected to it or outside the AS will be dropped. This situation is normally resolved, by configuring a virtual link from the ABR to the backbone area.
- ◆ In both the Cisco and IBM interpretation, a router connected to more than one area cannot issue a Type 1 router LSA declaring itself as an ABR unless it meets the other criteria listed above.

Routing table calculations are changed to allow the router to consider summary-LSAs from all attached areas if it is not an ABR, but has more than one attached area, or it does not have an active backbone connection.

In other words, inter-area routes are calculated by examining summary-LSAs. If the router is an ABR and has an active backbone connection, only backbone summary-LSAs are examined. Otherwise (when either the router is not an ABR or it has no active backbone connection), the router should consider summary-LSAs from all actively attached areas.

This ensures that the summary-LSAs originated by area border routers advertise only intra-area routes into the backbone if the router has an active backbone connection, and advertises both intra-area and inter-area routes into the other areas. Otherwise, the router only advertises intra-area routes into non-backbone areas.

EXAMPLE

```
Console(config-router)#abr-type ibm  
Console(config-router)#
```

max-current-dd This command sets the maximum number of neighbors with which the switch can concurrently exchange database descriptor (DD) packets. Use the **no** form to restore the default setting.

SYNTAX

max-current-dd *max-packets*

no max-current-dd

max-packets - The maximum number of neighbors with which the switch can concurrently send or receive DD packets. (Range: 1-65535)

COMMAND MODE

Router Configuration

DEFAULT SETTING

5

COMMAND USAGE

- ◆ This limit applies separately to the number of neighbors to which DD packets can be concurrently sent, and to the number of neighbors from which DD packets can be concurrently received.

EXAMPLE

```
Console(config-router)#maximum-current-dd 10  
Console(config-router)#
```

RELATED COMMANDS

[show ipv6 ospf \(900\)](#)

router-id This command assigns a unique router ID for this device within the autonomous system for the current OSPFv3 process. Use the **no** form to restore the default setting.

SYNTAX

router-id *ip-address*

no router-id

ip-address - Router ID formatted as an IPv4 address.

COMMAND MODE

Router Configuration

DEFAULT SETTING

None

COMMAND USAGE

- ◆ This command sets the router ID for the OSPF process specified in the [router ipv6 ospf](#) command.
- ◆ The router ID must be unique for every router in the autonomous system. (Note that the router ID can also be set to 255.255.255.255).
- ◆ If this router already has registered neighbors, the new router ID will be used when the router is rebooted, or manually restarted by entering the [no router ipv6 ospf](#) followed by the [router ipv6 ospf](#) command.
- ◆ If the priority values of the routers bidding to be the designated router or backup designated router for an area are equal, the router with the highest ID is elected.
- ◆ The current routing process will not be enabled until a Router ID is configured with this command.

EXAMPLE

```
Console(config-router)#router-id 10.1.1.1
Console(config-router)#
```

RELATED COMMANDS

[router ipv6 ospf \(882\)](#)

timers spf This command configures the delay after receiving a topology change and starting the shortest path first (SPF) calculation, and the hold time between making two consecutive SPF calculations. Use the **no** form to restore the default values.

SYNTAX

timers spf *spf-delay* *spf-holdtime*

no timers spf

spf-delay - The delay after receiving a topology change notification and starting the SPF calculation. (Range: 0-2147483647 seconds)

spf-holdtime - The minimum time between two consecutive SPF calculations. (Range: 0-2147483647 seconds)

COMMAND MODE

Router Configuration

DEFAULT SETTING

SPF delay: 5 seconds

SPF holdtime: 10 seconds

COMMAND USAGE

- ◆ Setting the SPF holdtime to 0 means that there is no delay between consecutive calculations.
- ◆ Using a low value for the holdtime allows the router to switch to a new path faster, but uses more CPU processing time.

EXAMPLE

```
Console(config-router)#timers spf 20  
Console(config-router)#
```

Route Metrics and Summaries

area default-cost This command specifies a cost for the default summary route sent into a stub from an Area Border Router (ABR). Use the **no** form to remove the assigned default cost.

SYNTAX

area *area-id* **default-cost** *cost*

no **area** *area-id* **default-cost**

area-id - Identifies the stub. (The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.)

cost - Cost for the default summary route sent to a stub.
(Range: 0-16777215)

COMMAND MODE

Router Configuration

DEFAULT SETTING

Default cost: 1

COMMAND USAGE

- ◆ If the default cost is set to "0," the router will not advertise a default route into the attached stub.

EXAMPLE

```
Console(config)#router ipv6 ospf tag 1
Console(config-router)#area 1 default-cost 1
Console(config-router)#
```

RELATED COMMANDS

[area stub \(852\)](#)

area range This command summarizes the routes advertised by an Area Border Router (ABR). Use the **no** form to disable this function.

SYNTAX

[no] area area-id range ipv6-prefix/prefix-length {advertise | not-advertise}

area-id - Identifies an area for which the routes are summarized. The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.

ipv6-prefix - A full IPv6 address including the network prefix and host address bits.

prefix-length - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the portion of the address to summarize).

advertise - Advertises the specified address range.

not-advertise - The summary is not sent, and the routes remain hidden from the rest of the network.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

- ◆ This command can be used to summarize intra-area routes and advertise this information to other areas through Area Border Routers (ABRs).

- ◆ If the network addresses within an area are assigned in a contiguous manner, the ABRs can advertise a summary route that covers all of the individual networks within the area that fall into the specified range using a single **area range** command.
- ◆ If routes are set to be advertised by this command, the router will issue a Type 3 summary LSA for each address range specified by this command.
- ◆ This router supports up to 64 summary routes for area ranges.

EXAMPLE

This example creates a summary address for all area routes in the range of 73::/8, or all IPv6 address that start with the first byte 73 (hexadecimal).

```
Console(config-router)#area 1 range 73::/8 advertise
Console(config-router)#
```

default-metric This command sets the default metric for external routes imported from other protocols. Use the **no** form to remove the default metric for the supported protocol types.

SYNTAX

default-metric *metric-value*

no default-metric

metric-value – Metric assigned to all external routes imported from other protocols. (Range: 0-16777214)

COMMAND MODE

Router Configuration

DEFAULT SETTING

20

COMMAND USAGE

- ◆ The default metric must be used to resolve the problem of redistributing external routes from other protocols that use incompatible metrics.
- ◆ This command does not override the metric value set by the [redistribute](#) command. When a metric value has not been configured by the [redistribute](#) command, the **default-metric** command sets the metric value to be used for all imported external routes.

EXAMPLE

```
Console(config-router)#default-metric 100
Console(config-router)#
```

RELATED COMMANDS

[redistribute \(889\)](#)

redistribute This command redistributes external routing information from other routing protocols and static routes into an autonomous system. Use the **no** form to disable this feature or to restore the default settings.

SYNTAX

redistribute {**connected** | **static**} [**metric** *metric-value*]
[**metric-type** *type-value*]

no redistribute {**connected** | **rip** | **static**} [**metric**] [**metric-type**]

connected - Imports all currently connected entries.

static - IPv6 static routes will be imported into this Autonomous System.

metric-value - Metric assigned to all external routes for the specified protocol. (Range: 0-16777214; Default: 20)

type-value

1 - Type 1 external route

2 - Type 2 external route (default) - Routers do not add internal route metric to external route metric.

COMMAND MODE

Router Configuration

DEFAULT SETTING

redistribution - none

metric-value - 20

type-metric - 2

COMMAND USAGE

- ◆ This command is used to import routes learned from other routing protocols into the OSPF domain, and to generate AS-external-LSAs.
- ◆ When you redistribute external routes into an OSPF autonomous system (AS), the router automatically becomes an autonomous system boundary router (ASBR).
- ◆ Metric type specifies the way to advertise routes to destinations outside the AS through External LSAs. When a Type 1 LSA is received by a router, it adds the internal cost to the external route metric. In other words, the cost of the route

from any router within the AS is equal to the cost associated with reaching the advertising ASBR, plus the cost of the external route. When a Type 2 LSA is received by a router, it only uses the external route metric to determine route cost.

EXAMPLE

This example redistributes automatically connected routes as Type 1 external routes.

```
Console(config-router)#redistribute connected metric-type 1
Console(config-router)#
```

Area Configuration

area stub This command defines a stub area. To remove a stub, use the **no** form without the optional keyword. To remove the summary attribute, use the **no** form with the summary keyword.

SYNTAX

[no] area area-id stub [no-summary]

area-id - Identifies the stub area. The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.

no-summary - Stops an Area Border Router (ABR) from sending summary link advertisements into the stub area.

COMMAND MODE

Router Configuration

DEFAULT SETTING

No stub is configured.

Summary advertisement are sent into the stub.

COMMAND USAGE

- ◆ All routers in a stub must be configured with the same area ID.
- ◆ Routing table space is saved by stopping an ABR from flooding Type-4 Inter-Area Router and Type 5 AS-External LSAs into the stub. Since no information on external routes is known inside the stub, an ABR will advertise the default route 0::0/0 using a Type 3 Inter-Area Prefix LSA.
- ◆ The default setting for this command blocks Type-4 Inter-Area Router and Type 5 AS-External LSAs. Therefore, any destinations that cannot be matched to an inter-area or intra-area route will have to use the default route.
- ◆ Use the **no-summary** parameter of this command on an ABR attached to the stub to define a totally stubby area, blocking all Type 3 network summary LSAs.

Define an area as a totally stubby area only if routers in the area do not require summary LSAs from other areas.

- ◆ Use the [area default-cost](#) command to specify the cost of a default summary route sent into a stub by an ABR attached to the stub area.

EXAMPLE

This example creates a stub area 2, and makes it totally stubby by blocking all Type 3 summary LSAs.

```
Console(config-router)#area 2 stub no-summary
Console(config-router)#
```

RELATED COMMANDS

[area default-cost \(886\)](#)

area virtual-link This command defines a virtual link. To remove a virtual link, use the **no** form with no optional keywords. To restore the default value for an attribute, use the **no** form with the required keyword.vvvv

SYNTAX

area *area-id* **virtual-link** *router-id*
 [**dead-interval** *seconds*] [**hello-interval** *seconds*]
 [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*]

no area *area-id* **virtual-link** *router-id*
 [**dead-interval** | **hello-interval** | **retransmit-interval** | **transmit-delay**]

area-id - Identifies the transit area for the virtual link. The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.

router-id - Router ID of the virtual link neighbor. This specifies the Area Border Router (ABR) at the other end of the virtual link. To create a virtual link, enter this command for an ABR at both ends of the link. One of the ABRs must be next to the isolated area and the transit area at one end of the link, while the other ABR must be next to the transit area and backbone at the other end of the link.

dead-interval *seconds* - Specifies the time that neighbor routers will wait for a hello packet before they declare the router down. This value must be the same for all routers attached to an autonomous system. (Range: 1-65535 seconds; Default: 4 x hello interval, or 40 seconds)

hello-interval *seconds* - Specifies the transmit delay between sending hello packets. Setting the hello interval to a smaller value can reduce the delay in detecting topological changes, but will increase the routing traffic. This value must be the same for all routers attached to an autonomous system. (Range: 1-65535 seconds; Default: 10 seconds)

retransmit-interval *seconds* - Specifies the interval at which the ABR retransmits link-state advertisements (LSA) over the virtual link. The retransmit interval should be set to a conservative value that provides an adequate flow of routing information, but does not produce unnecessary protocol traffic. However, note that this value should be larger for virtual links. (Range: 1-65535 seconds; Default: 5 seconds)

transmit-delay *seconds* - Estimates the time required to send a link-state update packet over the virtual link, considering the transmission and propagation delays. LSAs have their age incremented by this amount before transmission. This value must be the same for all routers attached to an autonomous system. (Range: 1-65535 seconds; Default: 1 second)

COMMAND MODE

Router Configuration

DEFAULT SETTING

area-id: None

router-id: None

hello-interval: 10 seconds

retransmit-interval: 5 seconds

transmit-delay: 1 second

dead-interval: 40 seconds

COMMAND USAGE

- ◆ All areas must be connected to a backbone area (0.0.0.0) to maintain routing connectivity throughout the autonomous system. If it not possible to physically connect an area to the backbone, you can use a virtual link. A virtual link can provide a logical path to the backbone for an isolated area, or can be configured as a backup connection that can take over if the normal connection to the backbone fails.
- ◆ A virtual link can be configured between any two backbone routers that have an interface to a common non-backbone area. The two routers joined by a virtual link are treated as if they were connected by an unnumbered point-to-point network.
- ◆ Any area disconnected from the backbone must include the transit area ID and the router ID for a virtual link neighbor that is adjacent to the backbone.

EXAMPLE

This example creates a virtual link using the defaults for all optional parameters.

```
Console(config-router)#area 3 virtual-link 192.168.0.9
Console(config-router)#
```

ipv6 router ospf area This command binds an OSPF area to the selected interface. Use the **no** form to remove an OSPF area, disable an OSPF process, or remove an instance identifier from an interface.

SYNTAX

[no] ipv6 router ospf area *area-id* [**tag** *process-name* | **instance-id** *instance-id*]

area-id - Area to bind to the current Layer 3 interface. An OSPF area identifies a group of routers that share common routing information. The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.

process-name - A process name must be entered when configuring multiple routing instances. (Range: Alphanumeric string up to 16 characters)

instance-id - Identifies a specific OSPFv3 routing process on the link-local network segment attached to this interface. (Range: 0-255)

COMMAND MODE

Interface Configuration

DEFAULT SETTING

None

COMMAND USAGE

- ◆ An area ID uniquely defines an OSPF broadcast area. The area ID 0.0.0.0 indicates the OSPF backbone for an autonomous system. Each router must be connected to the backbone via a direct connection or a virtual link.
- ◆ Set the area ID to the same value for all routers on a network segment.
- ◆ The *process-name* is only used on the local router to distinguish between different routing processes (and must be configured with the [router ipv6 ospf](#) command before using it in the **ipv6 router ospf area** command).
- ◆ The *instance-id* is used on the link-local network segment to distinguish between different routing processes running on the same link, and allows routers participating in a common routing process to form adjacencies and exchange routing information.
- ◆ The backbone (area 0.0.0.0) must be created before any other area.

EXAMPLE

This example creates the backbone 0.0.0.0.

```
Console(config)#router ipv6 ospf tag 0
Console(config-router)#router-id 192.168.0.2
Console(config-router)#exit
Console(config)#interface vlan 1
```

```
Console(config-if)#ipv6 router ospf area 0 tag 0 instance-id 0  
Console(config-if)#
```

RELATED COMMANDS

[router ipv6 ospf \(882\)](#)

[router-id \(885\)](#)

[ipv6 router ospf tag area \(894\)](#)

ipv6 router ospf tag area This command binds an OSPF area to the selected interface and process. Use the **no** form to remove the specified area from an interface.

[no] ipv6 router ospf tag *process-name* **area** *area-id*
[instance-id *instance-id*]

area-id - Area to bind to the current Layer 3 interface. An OSPF area identifies a group of routers that share common routing information. The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.

process-name - A process name used to distinguish between multiple routing instances configured on the local router. (Range: Alphanumeric string up to 16 characters)

instance-id - Identifies a specific OSPFv3 routing process on the link-local network segment attached to this interface. (Range: 0-255)

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

No areas are defined.

COMMAND USAGE

- ◆ An area ID uniquely defines an OSPF broadcast area. The area ID 0.0.0.0 indicates the OSPF backbone for an autonomous system. Each router must be connected to the backbone via a direct connection or a virtual link.
- ◆ Set the area ID to the same value for all routers on a network segment.
- ◆ The *process-name* is only used on the local router to distinguish between different routing processes (and must be configured with the [router ipv6 ospf](#) command before using it in this command).
- ◆ The *instance-id* is used on the link-local network segment to distinguish between different routing processes running on the same link, and allows routers participating in a common routing process to form adjacencies and exchange routing information.
- ◆ The backbone (area 0.0.0.0) must be created before any other area.

EXAMPLE

This example assigns area 0.0.0.1 to the currently selected interface under routing process "1."

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 router ospf tag 1 area 0.0.0.1
Console(config-if)#
```

RELATED COMMANDS

[router ipv6 ospf \(882\)](#)

[router-id \(885\)](#)

[ipv6 router ospf area \(893\)](#)

Interface Configuration

ipv6 ospf cost This command explicitly sets the cost of sending a protocol packet on an interface, where higher values indicate slower ports. Use the **no** form to restore the default value.

SYNTAX

ipv6 ospf cost *cost* [**instance-id** *instance-id*]

no ipv6 ospf cost [**instance-id** *instance-id*]

cost - Link metric for this interface. Use higher values to indicate slower ports. (Range: 1-65535)

instance-id - Identifies a specific OSPFv3 routing process on the link-local network segment attached to this interface. (Range: 0-255)

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

1

COMMAND USAGE

- ◆ The interface cost indicates the overhead required to send packets across a certain interface. This is advertised as the link cost in router link state advertisements.
- ◆ Routes are assigned a metric equal to the sum of all metrics for each interface link in the route.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 ospf cost 10
Console(config-if)#
```

ipv6 ospf dead-interval This command sets the interval at which hello packets are not seen before neighbors declare the router down. Use the **no** form to restore the default value.

SYNTAX

ipv6 ospf dead-interval *seconds* [**instance-id** *instance-id*]

no ipv6 ospf dead-interval [**instance-id** *instance-id*]

seconds - The maximum time that neighbor routers can wait for a hello packet before declaring the transmitting router down. This interval must be set to the same value for all routers on the network. (Range: 1-65535)

instance-id - Identifies a specific OSPFv3 routing process on the link-local network segment attached to this interface. (Range: 0-255)

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

40 seconds, or four times the interval specified by the [ipv6 ospf hello-interval](#) command.

COMMAND USAGE

The dead-interval is advertised in the router's hello packets. It must be a multiple of the hello-interval and be the same for all routers on a specific network.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 ospf dead-interval 50
Console(config-if)#
```

RELATED COMMANDS

[ipv6 ospf hello-interval \(897\)](#)

ipv6 ospf hello-interval This command specifies the interval between sending hello packets on an interface. Use the **no** form to restore the default value.

SYNTAX

ipv6 ospf hello-interval *seconds* [**instance-id** *instance-id*]

no ipv6 ospf hello-interval [**instance-id** *instance-id*]

seconds - Interval at which hello packets are sent from an interface. This interval must be set to the same value for all routers on the network. (Range: 1-65535)

instance-id - Identifies a specific OSPFv3 routing process on the link-local network segment attached to this interface. (Range: 0-255)

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

10 seconds

COMMAND USAGE

Hello packets are used to inform other routers that the sending router is still active. Setting the hello interval to a smaller value can reduce the delay in detecting topological changes, but will increase routing traffic.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 ospf hello-interval 5
Console(config-if)#
```

RELATED COMMANDS

[ipv6 ospf dead-interval \(896\)](#)

ipv6 ospf priority This command sets the router priority used when determining the designated router (DR) and backup designated router (BDR) for an area. Use the **no** form to restore the default value.

SYNTAX

ipv6 ospf priority *priority* [**instance-id** *instance-id*]

no ipv6 ospf priority [**instance-id** *instance-id*]

priority - Sets the interface priority for this router. (Range: 0-255)

instance-id - Identifies a specific OSPFv3 routing process on the link-local network segment attached to this interface. (Range: 0-255)

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

1

COMMAND USAGE

- ◆ A designated router (DR) and backup designated router (BDR) are elected for each OSPF area based on Router Priority. The DR forms an active adjacency to all other routers in the area to exchange routing topology information. If for any reason the DR fails, the BDR takes over this role.
- ◆ Set the priority to zero to prevent a router from being elected as a DR or BDR. If set to any value other than zero, the router with the highest priority will become the DR and the router with the next highest priority becomes the BDR. If two or more routers are tied with the same highest priority, the router with the higher ID will be elected.
- ◆ If a DR already exists for a network segment when this interface comes up, the new router will accept the current DR regardless of its own priority. The DR will not change until the next time the election process is initiated.
- ◆ Configure router priority for multi-access networks only and not for point-to-point networks.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 ospf priority 5
Console(config-if)#
```

ipv6 ospf retransmit-interval This command specifies the time between resending link-state advertisements (LSAs). Use the **no** form to restore the default value.

SYNTAX

ipv6 ospf retransmit-interval *seconds* [**instance-id** *instance-id*]

no ipv6 ospf retransmit-interval [**instance-id** *instance-id*]

seconds - Sets the interval at which LSAs are retransmitted from this interface. (Range: 1-65535)

instance-id - Identifies a specific OSPFv3 routing process on the link-local network segment attached to this interface. (Range: 0-255)

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

5 seconds

COMMAND USAGE

- ◆ A router will resend an LSA to a neighbor if it receives no acknowledgment after the specified retransmit interval. The retransmit interval should be set to a conservative value that provides an adequate flow of routing information, but does not produce unnecessary protocol traffic. Note that this value should be larger for virtual links.
- ◆ Set this interval to a value that is greater than the round-trip delay between any two routers on the attached network to avoid unnecessary retransmissions.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 ospf retransmit-interval 7
Console(config-if)#
```

ipv6 ospf transmit-delay This command sets the estimated time to send a link-state update packet over an interface. Use the **no** form to restore the default value.

SYNTAX

ipv6 ospf transmit-delay *seconds* [**instance-id** *instance-id*]

no ipv6 ospf transmit-delay [**instance-id** *instance-id*]

seconds - Sets the estimated time required to send a link-state update.
(Range: 1-65535)

instance-id - Identifies a specific OSPFv3 routing process on the link-local network segment attached to this interface. (Range: 0-255)

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

1 second

COMMAND USAGE

- ◆ LSAs have their age incremented by this delay before transmission. When estimating the transmit delay, consider both the transmission and propagation delays for an interface. Set the transmit delay according to link speed, using larger values for lower-speed links.
- ◆ If this delay is not added, the time required to transmit an LSA over the link is not taken into consideration by the routing process. On slow links, the router may send packets more quickly than devices can receive them. To avoid this

problem, use the transmit delay to force the router to wait a specified interval between transmissions.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 ospf transmit-delay 6
Console(config-if)#
```

passive-interface This command suppresses OSPF routing traffic on the specified interface. Use the **no** form to allow routing traffic to be sent and received on the specified interface.

SYNTAX

[no] passive-interface vlan *vlan-id* [*ipv6-address*]

vlan-id - VLAN ID. (Range: 1-4094)

ipv6-address - A full IPv6 address including the network prefix and host address bits.

COMMAND MODE

Router Configuration

DEFAULT SETTING

None

COMMAND USAGE

You can configure an OSPF interface as passive to prevent OSPF routing traffic from exiting or entering that interface. No OSPF adjacency can be formed if one of the interfaces involved is set to passive mode. The specified interface will appear as a stub in the OSPF domain. Also, if you configure an OSPF interface as passive where an adjacency already exists, the adjacency will drop almost immediately.

EXAMPLE

```
Console(config-router)#passive-interface vlan 1 73::9
Console(config-router)#
```

Display Information

show ipv6 ospf This command shows basic information about the routing configuration.

COMMAND MODE

Privileged Exec

EXAMPLE

```

Console#show ipv6 ospf
  Routing Process "ospf 1" with ID 192.168.0.2
  Process uptime is 24 minutes
  Supports only single TOS(TOS0) routes
  SPF schedule delay 5 secs, Hold time between two SPF's 10 secs
  Number of incoming concurrent DD exchange neighbors 0/5
  Number of outgoing concurrent DD exchange neighbors 0/5
  Number of external LSA 0. Checksum 0x000000
  Number of opaque AS LSA 0. Checksum 0x000000
  Number of LSA received 0
  Number of areas attached to this router: 2

    Area 0.0.0.0 (BACKBONE)
      SPF algorithm executed 2 times
      Number of LSA 1. Checksum 0x001aa9
    Area 0.0.0.1
      SPF algorithm executed 2 times
      Number of LSA 1. Checksum 0x001aa9

```

Console#

Table 191: show ip ospf - display description

Field	Description
<i>Routing Process</i>	
Routing Process	OSPF process name and router ID. The router ID uniquely identifies the router in the autonomous system. By convention, this is normally set to one of the router's IP interface addresses.
Process uptime	The time this process has been running
Supports only single TOS (TOS0) routes	Optional Type of Service (ToS) specified in OSPF Version 2, Appendix F.1.2 is not supported, so only one cost per interface can be assigned.
SPF schedule delay	The delay after receiving a topology change notification and starting the SPF calculation.
Hold time	Sets the hold time between two consecutive SPF calculations.
Number of concurrent DD exchange neighbors	Number of neighbors currently exchanging database descriptor packets.
Number of external LSA	The number of external link-state advertisements (Type 5 LSAs) in the link-state database. These LSAs advertise information about routes outside of the autonomous system.
Checksum	The sum of the LS checksums of the external link-state advertisements contained in the link-state database.
Number of opaque AS LSA	Number of opaque link-state advertisements (Type 9, 10 and 11 LSAs) in the link-state database. These LSAs advertise information about external applications, and are only used by OSPF for the graceful restart process.
Checksum	The sum of the LS checksums of opaque link-state advertisements contained in the link-state database.
Number of LSA received	The number of link-state advertisements that have been received.
Number of areas attached to this router	The number of configured areas attached to this router.

Table 191: show ip ospf - display description (Continued)

Field	Description
<i>Area Information</i>	
Area	The area identifier. Note that "(Inactive)" will be displayed if no IPv6 address has been configured on the interface.
SPF algorithm executed x times	The number of times the shortest path first algorithm has been executed for this area
Number of LSA	The total number of link-state advertisements in this area's link-state database, excluding AS External LSA's.
Checksum	The sum of the LS checksums of link-state advertisements for this network (area) contained in the link-state database.

show ipv6 ospf database This command shows information about different OSPF Link State Advertisements (LSAs) stored in this router's database.

SYNTAX

show ipv6 ospf [tag process-id] database

process-id - The ID of the router process for which information will be displayed. (Range: 1-10)

COMMAND MODE

Privileged Exec

EXAMPLES

The following shows output for the **show ip ospf database** command.

```

Console#show ipv6 ospf database

OSPF Router with ID (192.168.0.2) (TAG: 1)

Link-LSA
Link State ID  ADV Router  Age  Seq#          CkSum  Link
1001           192.168.0.2    71  0x80000001  0x06b7  0

Router-LSA (Area 0)
Link State ID  ADV Router  Age  Seq#          CkSum
0             192.168.0.2    31  0x80000002  0x14b1

AS-external-LSA
Link State ID  ADV Router  Age  Seq#          CkSum
Console#

```

Table 192: show ip ospf database - display description

Field	Description
OSPF Router Process with ID	OSPF router ID and process ID. The router ID uniquely identifies the router in the autonomous system. By convention, this is normally set to one of the router's IP interface addresses.
Link State ID	This field identifies the piece of the routing domain that is being described by the advertisement.
ADV Router	Advertising router ID
Age	Age of LSA (in seconds)
Seq#	Sequence number of LSA (used to detect older duplicate LSAs)
CkSum	Checksum of the complete contents of the LSA
Link	Number of interfaces attached to the router

show ipv6 ospf interface This command displays summary information for OSPF interfaces.

SYNTAX

show ipv6 ospf interface [vlan *vlan-id*]

vlan-id - VLAN ID (Range: 1-4094)

COMMAND MODE

Privileged Exec

EXAMPLE

```

Console#show ipv6 ospf interface vlan 1
VLAN 1 is up, line protocol is up
Link local Address FE80::200:E8FF:FE93:82A0/64, Area 0.0.0.0
Tag 1, Router ID 192.168.0.2, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 192.168.0.2, Interface Address
FE80::200:E8FF:FE93:82A0
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Neighbor Count is 0, Adjacent neighbor count is 0
Hello received 0 sent 92, DD received 0 sent 0
LS-Req received 0 sent 0, LS-Upd received 0 sent 0
LS-Ack received 0 sent 0, Discarded 0
Console#

```

Table 193: show ip ospf interface - display description

Field	Description
VLAN	VLAN ID and Status of physical link
Link local Address	Link local address of OSPF interface
Area	OSPF area to which this interface belongs
Tag	OSPF process identifier string

Table 193: show ip ospf interface - display description (Continued)

Field	Description
Router ID	Identifier for this router
Network Type	Includes broadcast, non-broadcast, or point-to-point networks
Cost	Interface transmit cost
Transmit Delay	Interface transmit delay (in seconds)
State	<ul style="list-style-type: none"> ◆ Backup – Backup Designated Router ◆ Down – OSPF is enabled on this interface, but interface is down ◆ DR – Designated Router ◆ DROther – Interface is on a multiaccess network, but is not the DR or BDR ◆ Loopback – This is a loopback interface ◆ PointToPoint – A direct link between two routers. ◆ Waiting – Router is trying to find the DR and BDR
Priority	Router priority
Designated Router	Designated router ID and respective interface address
Backup Designated Router	Backup designated router ID and respective interface address
Timer intervals	Configuration settings for timer intervals, including Hello, Dead and Retransmit
Neighbor Count	Count of network neighbors and adjacent neighbors
Hello	Number of Hello LSAs received and sent
DD	Number of Database Descriptor packets received and sent
LS-Req	Number of LSA requests
LS-Upd	Number of LSA updates
LS-Ack	Number of LSA acknowledgements
Discarded	Number of LSAs discarded

show ipv6 ospf neighbor This command displays information about neighboring routers on each interface within an OSPF area.

SYNTAX

show ipv6 ospf [tag process-id] neighbor

process-id - The ID of the router process for which information will be displayed. (Range: 1-10)

COMMAND MODE

Privileged Exec

EXAMPLE

```

Console#show ipv6 ospf neighbor

      ID          Pri      State      Interface ID      Interface
-----
  192.168.0.2      1      FULL/DR      1001      vlan1
Console#

```

Table 194: show ipv6 ospf neighbor - display description

Field	Description
ID	Neighbor's router ID
Pri	Neighbor's router priority
State	OSPF state and identification flag States include: Down – Connection down Attempt – Connection down, but attempting contact (for non-broadcast networks) Init – Have received Hello packet, but communications not yet established Two-way – Bidirectional communications established ExStart – Initializing adjacency between neighbors Exchange – Database descriptions being exchanged Loading – LSA databases being exchanged Full – Neighboring routers now fully adjacent Identification flags include: D – Dynamic neighbor S – Static neighbor DR – Designated router BDR – Backup designated router
Interface ID	
Interface	The interface to which this neighbor is attached

show ipv6 ospf route This command displays the OSPF routing table.

SYNTAX

show ipv6 ospf [tag process-id] route

process-id - The ID of the router process for which information will be displayed. (Range: 1-10)

COMMAND MODE

Privileged Exec

EXAMPLE

```

Console#show ipv6 ospf route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
C      ::1/128, lo0

```

```
O    2001:DB8:2222:7272::/64, VLAN1
C    2001:DB8:2222:7272::/64, VLAN1
?    FE80::/64, VLAN1 inactive
C    FE80::/64, VLAN1
?    FF00::/8, VLAN1 inactive
```

Console#

show ipv6 ospf virtual-links This command displays detailed information about virtual links.

SYNTAX

show ipv6 ospf [*tag process-id*] **virtual-links**

process-id - The ID of the router process for which information will be displayed. (Range: 1-10)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ipv6 ospf virtual-links
Virtual Link VLINK1 to router 192.168.0.2 is up
  Transit area 0.0.0.1 via interface VLAN1
  Local address 192.168.0.3
  Remote address 192.168.0.2
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
  Adjacency state Full
Console#
```

Table 195: show ipv6 ospf virtual-links - display description

Field	Description
Virtual Link to router	OSPF neighbor and link state (up or down)
Transit area	Common area the virtual link crosses to reach the target router
Local address	The IP address of ABR that serves as an endpoint connecting the isolated area to the common transit area.
Remote address	The IP address this virtual neighbor is using. The neighbor must be an ABR at the other endpoint connecting the common transit area to the backbone itself.
Transmit Delay	Estimated transmit delay (in seconds) on the virtual link
Timer intervals	Configuration settings for timer intervals, including Hello, Dead and Retransmit

Table 195: show ipv6 ospf virtual-links - display description (Continued)

Field	Description
Hello due	The timeout for the next hello message from the neighbor
Adjacency state	The adjacency state between these neighbors: Down – Connection down Attempt – Connection down, but attempting contact (for non-broadcast networks) Init – Have received Hello packet, but communications not yet established Two-way – Bidirectional communications established ExStart – Initializing adjacency between neighbors Exchange – Database descriptions being exchanged Loading – LSA databases being exchanged Full – Neighboring routers now fully adjacent

RELATED COMMANDS

[area virtual-link \(891\)](#)

BORDER GATEWAY PROTOCOL (BGPv4)

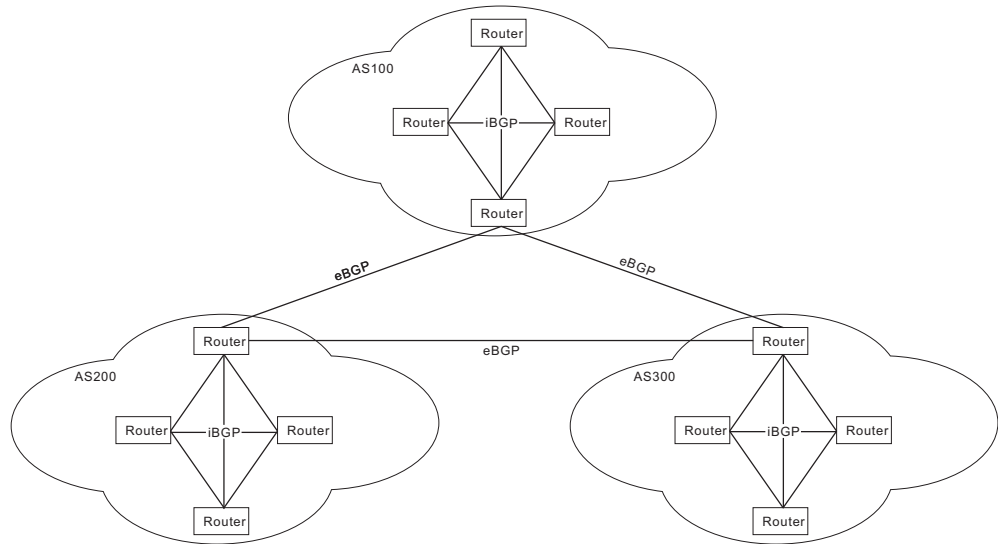
BGP OVERVIEW An autonomous system (AS) functions as a separate routing domain under one administrative authority, which implements its own routing policies. An AS exchanges routing information within its boundaries using Interior Gateway Protocols (IGPs) such as RIP or OSPF, and connects to external organizations or to the Internet using an Exterior Gateway Protocol (EGP). BGP version 4 is the primary EGP deployed on the Internet today.

A communication session must be maintained between bordering ASs to support the periodic exchange of routing information. One of the major design choices for BGP is the use of a TCP connection to exchange routing information between peers. Exchanging connectivity information over a reliable transport mechanism effectively delegates all error control functions to TCP.

The other major innovation for BGP is the use of path vectors which carry the full list of transit networks, or ASs, traversed between the source and destination. Loops are prevented simply by checking the path vector to see if same AS is listed twice. This approach solves many of the scalability problems encountered when applying distance-vector or link-state methods to make routing decisions in complex topologies.

EXTERNAL AND INTERNAL BGP When connecting to the Internet, external BGP (eBGP) is used. Although BGP is widely used as an exterior gateway protocol (EGP), it is also used in many organizations with complex internal networks. Internal networks can be simplified by exchanging routing information among BGP peers within the same organization through internal BGP (iBGP) peering sessions.

Figure 6: Connections for Internal and External BGP



External BGP – eBGP interconnects different ASs through border routers, or eBGP peers. These peering routers are commonly connected over a WAN link using a single physical path. Alternatively, multiple eBGP peer connections may be used to provide redundancy or load balancing. Distinct BGP sessions are used between redundancy peers to ensure that if one session fails, another will take over.

BGP uses the AS path attribute to record the ASs that must be followed to reach the prefix for a network aggregate. When a prefix is announced to an eBGP peer, the local AS number is prepended to the AS path. This prevents routing loops by rejecting any prefix announcements that include the local AS number in the AS path. These announcements are also used by eBGP in the best path selection process.

eBGP speakers, can communicate with other external peers or with iBGP peers. A BGP speaker can determine if it is communicating with an external or internal peer by comparing the AS number sent in OPEN messages by a peer with that of its own internal value. If it matches, then this neighbor is an iBGP speaker, and if it does not, then it is an eBGP speaker. An eBGP speaker can advertise prefixes it has learned from another eBGP speaker to a neighboring iBGP speaker; and it can also advertise prefixes it has learned from an iBGP speaker to an eBGP speaker.

Internal BGP – In contrast to eBGP peers which have different AS numbers, iBGP peers are configured with the same AS number. All iBGP peers within the same AS should be connected to one another in a full-mesh connection (except when using route reflection). When a prefix is announced from one iBGP peer to another, the AS path is not changed. Since all iBGP peers are fully meshed, they will have the same information in their BGP table, unless routing policies have been modified for some of the peers.

When a iBGP peer receives a prefix announcement, it uses the best path selection algorithm to see if the received announcement is the best path for that prefix. If it is, the peer inserts this route into its routing table, and announces it to all of its peers, both iBGP and eBGP. If it is not the best available path, the peer keeps a copy of it in its routing table so that if path information for that prefix changes (such as if the

current best available path is withdrawn), it can be used to calculate a new best available path.

BGP cannot detect routes and provide reachability information. To ensure that each iBGP peer knows how to reach other, each peer must run some sort of Interior Gateway Protocol (such as static routes, direct routes, RIP or OSPF) which provides neighbor IP addresses. In order to avoid routing loops, an iBGP speaker cannot advertise prefixes it has learned from one iBGP peer to another neighboring iBGP peer.

BGP ROUTING BASICS

Both RIP and OSPF attach a metric, or cost, to each path. These protocols rely on every router attaching the same meaning to each metric, allowing consistent calculation of routes. However, after routing policies are put in place, routers may value some metrics differently, invalidating the basic assumptions upon which RIP and OSPF are based. This makes it unrealistic to run a distance-vector AS-level protocol

BGP uses a path vector routing approach, which is roughly based on a distance-vector approach, where the cost between two adjacent ASes is implicitly assumed to be a single hop. The shortest path from an AS to a remote AS is therefore the path with the shortest number of AS hops. Just note that each AS may be comprised of multiple routers or networks that a packet traverses as it crosses the associated route to the destination, so the AS hop count does not equal to the number of routers along that path.

PATH ATTRIBUTES

The key information passed along with the path vector in routing messages include the following attributes:

- ◆ **ORIGIN** – This attribute indicates how the network of BGP routers first learned of a route, and is set by the first BGP router to introduce the routes to its peers. There are three methods for injecting a prefix into an update message: IGP, EGP and Incomplete.
- ◆ **AS_PATH** – This attribute lists the autonomous systems that make up the path to the routes' destination. Each entry contains a series of path segments. Each path segment begins with a 1 for SETS or a 2 for SEQUENCES, where a SET indicates that it is an aggregate prefix which was derived from multiple ASes.
- ◆ **NEXT_HOP** – This attribute indicates the IP address of the router that should be used as the next hop to reach the router's destination. This address is normally that of the router sending the BGP message, but a BGP router may advertise a route on behalf of another router.
- ◆ **MULTI_EXIT_DISC (MED)** – The multi-exit discriminator attribute lets an autonomous system set a preference for different routes when there are multiple external links to a neighboring AS. Selection is normally based on the exit point with the lowest metric.

- ◆ **WEIGHT** – This attribute is used locally by a router to select a path when multiple paths are available for a prefix.
- ◆ **LOCAL_PREF** – This local preference attribute is similar to that of the MED, but within an AS. It sets a metric which is used between BGP speakers within an AS. It can help in selecting an outgoing BGP when an AS has connectivity to multiple ASes or multiple BGP routes even with the same next hop AS.
- ◆ **ATOMIC_AGGREGATE** – This attribute indicates that the routes were created by aggregating more specific routes. More specific routes may exist for some of these longer prefixes, but the router chose not to send them, so as to reduce the size for the AS path parameters.
- ◆ **AGGRATOR** – This is an optional attribute that identifies the AS and router that originally aggregated the routes.
- ◆ **COMMUNITY** – This attribute associates routing information with a community of users. These communities share a common property, and tagging routes with a community makes it easier for routers to identify that property and enforce appropriate routing policies.
- ◆ **ORIGINATOR_ID** – This attribute is included when a route reflector reflects a route. Then if the reflector later receives a route with its own originator ID, a potential routing loop can be broken.
- ◆ **CLUSTER_LIST** – This attribute is of a list of the clusters through which a route has been reflected. Every route reflector adds its own cluster ID to the list. If the reflector receives a route with its own cluster ID, a potential routing loop can be broken.
- ◆ **MP_REACH_NLRI** – This attribute describes routes for network protocols other than IPv4. The attribute identifies the protocol with an address family identifier (AFI) and a subsequent address family identifier (SAFI). It contains the address of the next hop router for the destinations, as well as the link level (e.g., Ethernet) addresses for that next hop. It concludes with the destinations expressed as prefixes.
- ◆ **MP_UNREACH_NLRI** – This attribute withdraws non-IPv4 routes. It includes the route's AFI, SAFI, and network address prefixes.
- ◆ **EXTENDED-COMMUNITIES** – This attribute provides a mechanism for labeling various information carried in route advertisements. It provides an extended type field to ensure that communities can be assigned for a broad range of uses, without fear of overlap.

PATH SELECTION

When there are multiple paths to the same prefix (with the same prefix length), the information included in route advertisement is used to select the best path to a destination following the rules shown below.

1. Choose the path with the highest WEIGHT. If the value of this attribute is the same for more than one candidate, go to the next step.
2. Choose the path with the highest LOCAL-PREF. If the value of this attribute is the same for more than one candidate, go to the next step.
3. Choose the path that was generated by the local router with the `network` or `aggregate-address` command. If the value of this criteria is the same for more than one candidate, go to the next step.
4. Choose the path with the shortest AS_PATH. If the value of this attribute is the same for more than one candidate, go to the next step. Note that this attribute may be disabled in the selection process using the `bgp bestpath as-path ignore` command.
5. Choose the path with the lowest ORIGIN (IGP < EGP < Incomplete). If the value of this criteria is the same for more than one candidate, go to the next step.
6. Choose the path with the lowest MED. By default, the MED attribute is considered only when a prefix is received from neighbors in the same AS. If the value of this criteria is the same for more than one candidate, go to the next step.
7. Choose an eBGP path over an outer confederation, and an outer confederation over an iBGP path. If the value of this criteria is the same for more than one candidate, go to the next step.
8. Choose the path with the lowest IGP metric to the next hop. If the value of this criteria is the same for more than one candidate, go to the next step.
9. Choose the path originated by the BGP router with the lowest router ID.

MESSAGE TYPES

Four message types are used by BGP. The OPEN message is used by BGP peers to identify their capabilities, the UPDATE message is used to advertise/withdraw prefixes, the NOTIFICATION message is used to send errors or close the session, and the KEEPALIVE messages is used to keep the BGP session up. These message types are described below.

- ◆ OPEN – BGP routers normally wait for BGP connections on TCP port 179. A router that wants to establish an association will first open a TCP connection leading to that port on the peer router. Once the connection has been set, each side sends an OPEN message to negotiate the association's parameters based on the capabilities advertised in these messages. Open messages include information about the BGP version number in use, the peer's AS number, the hold time, the BGP identifier (i.e., loopback address or the highest value of all the BGP speaker's interfaces), and optional parameter length.

- ◆ **UPDATE** – These messages are used to announce or withdraw IP prefixes, and include the following components: withdrawn route length, withdrawn routes, total path attributes length, path attributes, and network layer reachability information.
- ◆ **NOTIFICATION** – These messages are used to indicate error conditions. The underlying TCP session is closed after a notification message is sent.
- ◆ **KEEPALIVE** – These messages are sent at a set interval and are used to verify that the BGP session is active. The hold timer is reset upon receipt of a KEEPALIVE or UPDATE message. If the hold time is set to zero by both peers, a BGP session can be kept open without generating KEEPALIVE messages.

ROUTE AGGREGATION AND DISSEMINATION

In the Internet, the number of destinations is larger than most routing protocols can manage. It is not possible for routers to track every possible destination in their routing tables. To overcome this problem BGP relies on route aggregation, whereby multiple destinations are combined in a single advertisement. Routers receiving this information, treat the combined destinations as a single destination, thus reducing the number of individual routes that must be remembered. This also reduces the network overhead required to transmit update packets and maintain routing tables.

In BGP, route aggregation combines the address blocks for networks from two or more ASes into a supernet, and transmits this information to a downstream AS. This supernetted address block is less specific, and only lists the AS number of the AS where the supernetting was done. The Atomic_Aggregate attribute indicates that attributes for more specific paths are not included in the aggregated route, and the Aggregator attribute indicates the AS and router where the aggregation was done. The aggregator node will now serve as a proxy, using the more specific routes it still maintains in its own routing table.

After inbound routes have been aggregated, the BGP speaker can propagate this information based on export policies for individual neighbors or for defined router groups, using route maps or other more precise routing criteria.

INTERNAL BGP SCALABILITY

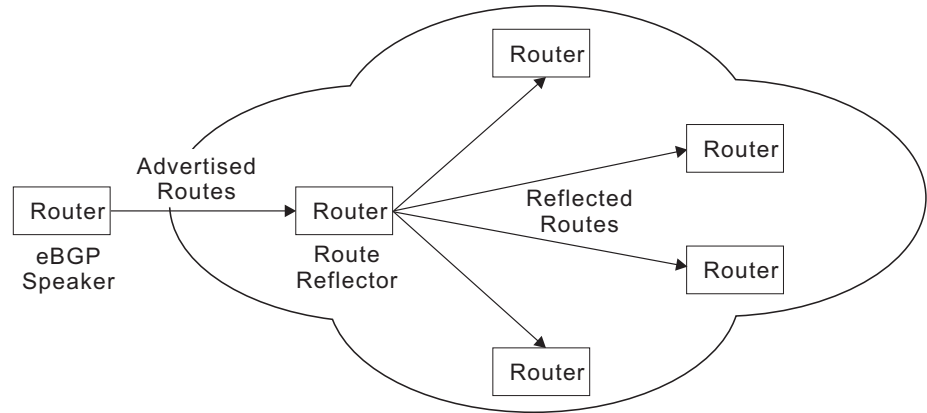
An iBGP speaker cannot advertise IP prefixes it has learned from one iBGP speaker to another neighboring iBGP speaker. iBGP therefore requires full-mesh connectivity among all iBGP speakers. For local networks containing a large number of speakers, this requirement may be difficult to meet. There are several commonly used approaches to resolving this problem, including route reflectors, confederations, and route servers.

ROUTE REFLECTORS

Route reflection designates one or more iBGP speakers as router concentrators or route reflectors, which are allowed to re-advertise routing information within the same autonomous system. It also clusters a subset of iBGP speakers with each route reflector (also known as route reflector clients), and adds several new attributes to

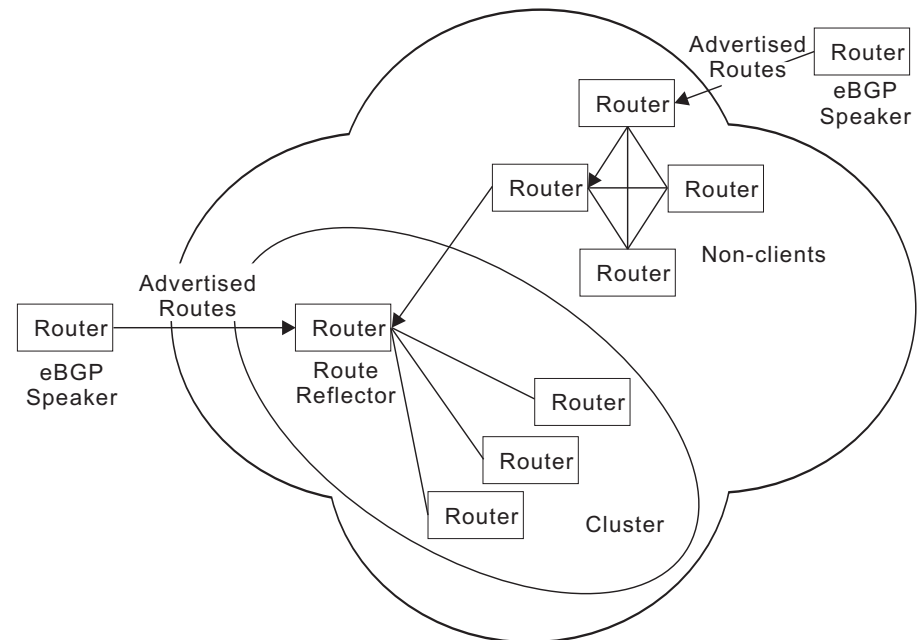
help detect routing loops. Using the cluster hierarchy, connections are only required between the route reflector and its clients, overcoming the normal requirement for full-mesh connectivity among all iBGP speakers.

Figure 7: Connections for Single Route Reflector



Route reflector clients are not aware that they are connected to a route reflector, and function as though fully meshed within the autonomous system. For redundancy, a cluster may contain more than one route reflector. Each cluster is identified a Cluster-ID. When there is only one route reflector in a cluster, the Cluster-ID is the BGP identifier of the route reflector. If there is more than one route reflector in a cluster, a common identifier can be defined for use by all route reflectors in the cluster.

Figure 8: Connections for Multiple Route Reflectors



If there is only one route reflector in a cluster, that router would still have to process the same number of routing messages that would be required if it were in a fully meshed network. It is therefore preferable to use more than one route reflector in a

cluster to reduce the overall number of iBGP sessions a single reflector has to handle.

If multiple route reflectors are configured in the same cluster, they must be fully meshed with each other. However, the route reflector clients only need to be connected to its designated route reflector. Once all iBGP routing sessions are established, routing advertisements must follow these rules:

- ◆ Announcements received by a route reflector from another reflector are passed to its clients.
- ◆ Announcements received by a route reflector from a reflector client are passed to other route reflectors in the cluster.
- ◆ Announcements received by a route reflector from an eBGP speaker are passed to all route reflectors in the cluster and to its own clients.

It can now be seen that routing information learned from an iBGP speaker can be passed to another iBGP speaker. This breaks the normal rules for a fully meshed iBGP autonomous system, and other steps are now required to avoid routing loops. These include the addition of the following new attributes:

- ◆ Originator-ID – When a route reflector learns about a route from one of its clients, it adds this attribute to the announcement before reflecting it to other speakers. If a route reflector receives an announcement about a route with an Originator-ID that matches its own router ID, it should drop it.
- ◆ Cluster-List – This is a list of the clusters through which a route announcement has passed. When a route reflector passes on an announcement, it must prepend the local Cluster-ID to this list. The Cluster-List thereby serves a similar function to the AS-Path attribute in detecting routing loops.

Configuration Guidelines

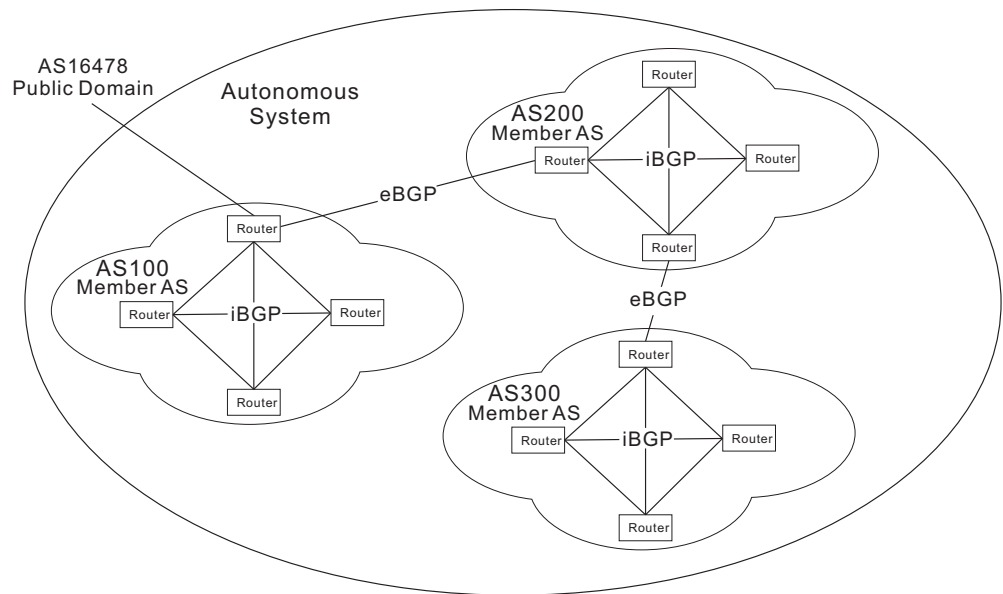
1. Route reflection from this router is enabled by default. If it has been disabled, use the `bgp client-to-client reflection` command to restore route reflection via this router.
2. If more than one route reflector is used, use the `bgp cluster-id` command to configure the cluster identifier.
3. Use the `neighbor route-reflector-client` command configure a neighboring router as a client.

CONFEDERATIONS

Confederations simply divides an autonomous system into smaller groups. It splits up an AS into multiple sub-ASes, where full mesh connections are maintained only within each sub-As, and sub-ASes are connected by eBGP. The overall AS is known as a confederation, while the sub-ASes may also be referred to as member ASes.

The entire confederation has a unique AS number, while the member ASes may have AS numbers obtained from public AS number space, or use AS number from private AS number space.

Figure 9: Connections for BGP Confederation



To prevent looping within the confederation, the AS-Confed-Set and AS-Confed-Sequence path attributes are added. These attributes function in the same manner as AS-Set and AS-Sequence. The following additional requirements are applied for route advertisements passed between member ASes:

- ◆ The Local-Pref for a route may be passed from one member AS to another member AS. This exception to normal practice is allowed within the confederation since this attribute is meant for use by the entire AS.
- ◆ The Next-Hop for a route set by the first BGP speaker in the confederation may be passed from one member AS to another member.
- ◆ When a route advertisement is passed from one member AS to another, the AS-Confed-Sequence must be inserted into the AS-Path along with the AS number of the member AS to help prevent looping.

Border routers that also peer with outside ASes have to modify routing information that leaves the confederation so that the internal structure of the confederation remains hidden to exterior peers, primarily because this information is of no use to another external AS. The information stripped from route advertisements and update messages sent outside of the confederation include AS-Confed-Sequence and AS-Confed-Set. Neither are AS numbers of member ASes advertised to exterior peers.

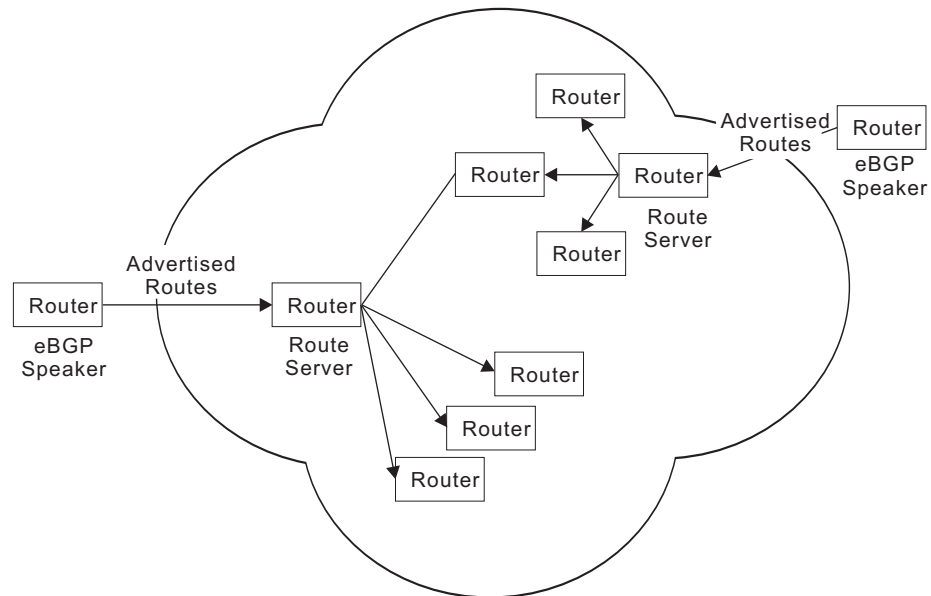
Configuration Guidelines

1. Use the `bgp confederation identifier` command to configure the identifier for a confederation containing smaller multiple internal autonomous systems.
2. Use the `bgp confederation peer` command to add an internal peer autonomous system to a confederation.

ROUTE SERVERS

Route Servers are used to relay routes received from remote ASes to client routers, as well as to relay routes between client routers. Clients maintain BGP sessions only with the assigned route servers. Sessions with more than one server can be used to provide redundancy and load sharing. All routes received from a client router are propagated to other clients through the Route Server. Since all external routes and their attributes are relayed unmodified between client routers, they acquire the same routing information as they would via direct peering in a full mesh configuration.

Figure 10: Connections for Route Server



Configuration Guidelines

Use the `neighbor route-server-client` command to configure this router as a route server and the specified neighbor as its client.

ROUTE FLAP DAMPENING

An update message is sent from a BGP speaker to a neighboring speaker whenever any change to a route occurs. A speaker announcing such a route is also responsible for any changes, including withdrawal, change in AS-Path or Next-Hop, to the same neighbor, irrespective of where the change was learned. In practice this may cause a BGP speaker to announce a new route, and then almost immediately withdraw or update the route a few seconds later, repeatedly. Since routing

information is propagated to other downstream speakers, there is a ripple effect that creates a cascading storm of updates through the ASes. This causes instability in the routing tables, as well as the computational overhead required to compute the best path, and an increase in convergence time.

Route damping provides a relief mechanism to minimize the effects of route flapping. It can reduce the propagation of updates for flapping routes without impacting the route convergence time for stable routes. When enabled, a route is assigned a penalty each time it flaps (i.e., announced and then quickly withdrawn). If the penalty exceeds 2000 (the suppress limit) the route is suppressed. After the route remains stable for a specified interval (half-life), the penalty is reduced by half. Subsequently, the penalty is reduced every 15 minutes. When the penalty falls below a specified value (reuse limit), the route is unsuppressed.

The penalty never exceeds the maximum penalty, which is computed from specified attributes as shown below:

$$\text{Maximum penalty} = \text{reuse-limit} * 2^{(\text{max-suppress-time}/\text{half-life})}$$

When a route is being “damped,” any updates or withdrawals for this route received from a peer are ignored. This limits the effects of route flapping to a single peering connection. Since most ASes are connected by high-speed links, it is not always necessary to use route damping. However, when invoked, it may be necessary to fine tune the penalty attributes to ensure fair treatment to unstable routes.

Configuration Guidelines

1. Use the **bgp damping** command to enable route damping.
2. Use the **bgp damping** command to adjust the penalty attributes of *half-life*, *reuse-limit*, *suppress-limit*, and *max-suppress-time*.
3. Use the **clear ip bgp damping** command to clear route damping information and unsuppresses any suppressed routes.

BGP COMMAND LIST

Table 196: Border Gateway Protocol Commands – Version 4

Command	Function	Mode
<i>General Configuration</i>		
router bgp	Enables BGPv4 routing process and enters router configuration mode	GC
ip as-path access-list	Configures an autonomous system path access list	GC
ip community-list	Configures a community list	GC
ip extcommunity-list	Configures an extended community list	GC
ip prefix-list	Configures an address prefix list	GC
aggregate-address	Configures an aggregate address in the routing table	RC
bgp client-to-client reflection	Configures route reflection between clients via route reflector	RC

Table 196: Border Gateway Protocol Commands – Version 4 (Continued)

Command	Function	Mode
<code>bgp cluster-id</code>	Configures cluster identifier for multiple route reflectors in the same cluster	RC
<code>bgp confederation identifier</code>	Configures the identifier for a confederation containing smaller multiple internal autonomous systems	RC
<code>bgp confederation peer</code>	Adds an internal peer autonomous system to a confederation	RC
<code>bgp dampening</code>	Configures route dampening to reduce the propagation of unstable routes	RC
<code>bgp enforce-first-as</code>	Denies an update received from an external peer that does not list its own autonomous system number at the beginning of the AS path attribute	RC
<code>bgp fast-external-failover</code>	Resets sessions for any directly connected external peers if the link goes down	RC
<code>bgp log-neighbor-changes</code>	Enables logging of neighbor resets (that is, up or down status changes)	RC
<code>bgp network import-check</code>	Checks the existence of the next-hop and its accessibility to IGP	RC
<code>bgp router-id</code>	Sets the router ID for this device	RC
<code>bgp scan-time</code>	Sets the interval at which to validate next hop information for BGP routes	RC
<code>network</code>	Specifies a network to advertise	RC
<code>redistribute</code>	Redistribute routes from one routing domain to another	RC
<code>timers bgp</code>	Sets the Keep Alive time used for maintaining connectivity, and the Hold time to wait for Keep Alive messages before declaring a neighbor down	RC
<code>clear ip bgp</code>	Clears connections using hard or soft re-configuration	PE
<code>clear ip bgp dampening</code>	Clears route dampening information and unsuppresses any suppressed routes	PE
<i>Route Metrics and Selection</i>		
<code>bgp always-compare-med</code>	Allows comparison of the Multi Exit Discriminator (MED) for paths advertised from neighbors in different autonomous systems	RC
<code>bgp bestpath as-path ignore</code>	Ignores AS path length in the selection of a path	RC
<code>bgp bestpath compare-confed-aspath</code>	Compare confederation AS path length in addition to external AS path length in the selection of a path	RC
<code>bgp bestpath compare-routerid</code>	Compare similar routes from external peers, and give preference to a route with the lowest router identifier	RC
<code>bgp bestpath med</code>	Enables comparison of MED attribute for paths learned from confederation peers, and the treatment of a route when the MED is missing	RC
<code>bgp default local-preference</code>	Sets the default local preference used for best path selection among local iBGP peers	RC
<code>bgp deterministic-med</code>	Enforces deterministic comparison of the MED attribute between all paths received from the same AS, ensuring that selection of the best path will always be the same, regardless of the order in which the paths are received by the local router	RC

Table 196: Border Gateway Protocol Commands – Version 4 (Continued)

Command	Function	Mode
<code>distance</code>	Sets the administrative distance for a specified external BGP (eBGP) route	RC
<code>distance bgp</code>	Sets the administrative distance for BGP external, internal, and local routes	RC
<i>Neighbor Configuration</i>		
<code>neighbor activate</code>	Enables exchange of routing information with a neighboring router or peer group	RC
<code>neighbor advertisement-interval</code>	Configures the interval between sending update messages to a neighbor	RC
<code>neighbor allowas-in</code>	Configures the number of times the AS path for a received route can contain the same AS number	RC
<code>neighbor attribute-unchanged</code>	Configures certain attributes to be kept unchanged for transparent transmission to the specified neighbor	RC
<code>neighbor capability dynamic</code>	Configures dynamic negotiation of capabilities between neighboring routers	RC
<code>neighbor capability orf prefix-list</code>	Configures negotiation of outbound route filter capabilities with neighboring router	RC
<code>neighbor default-originate</code>	Allows the local router to send a default route to a neighbor	RC
<code>neighbor description</code>	Configures the description of a neighbor or peer group	RC
<code>neighbor distribute-list</code>	Filters route updates to/from a neighbor or peer group	RC
<code>neighbor dont-capability-negotiate</code>	Disables capability negotiation when creating connections	RC
<code>neighbor ebgp-multihop</code>	Allows eBGP neighbors to exist in different segments, and configures the maximum hop count (TTL)	RC
<code>neighbor enforce-multihop</code>	Enforces the requirement for all neighbors to form multi-hop connections	RC
<code>neighbor filter-list</code>	Filters route updates sent to or received from a neighbor based on an AS path access-list	RC
<code>neighbor interface</code>	Specifies the interface to a neighbor	RC
<code>neighbor maximum-prefix</code>	Sets the maximum number of route prefixes that can be received from a neighbor	RC
<code>neighbor next-hop-self</code>	Configures the local router as the next hop for a neighbor	RC
<code>neighbor override-capability</code>	Overrides the result of capability negotiations, allowing a session to be formed with a peer that does not support capability negotiation	RC
<code>neighbor passive</code>	Passively forms a connection with the specified neighbor, not sending a TCP connection request, but waiting a request from the specified neighbor	RC
<code>neighbor peer-group (Creating)</code>	Configures a router peer group which can be easily configured with the same attributes	RC
<code>neighbor peer-group (Group Members)</code>	Assigns routers to a peer group	RC
<code>neighbor port</code>	Specifies the TCP port number of the partner through which communications are carried	RC
<code>neighbor prefix-list</code>	Configures prefix restrictions applied in inbound/outbound route updates to/from specified neighbors	RC

Table 196: Border Gateway Protocol Commands – Version 4 (Continued)

Command	Function	Mode
<code>neighbor remote-as</code>	Configures a neighbor and its AS number, identifying the neighbor as a local AS member	RC
<code>neighbor remove-private-as</code>	Removes private autonomous system numbers from outbound routing updates to an external neighbor	RC
<code>neighbor route-map</code>	Specifies the route mapping policy for inbound/outbound routing updates for specified neighbors	RC
<code>neighbor route-reflector-client</code>	Configures this router as a route reflector and the specified neighbor as its client	RC
<code>neighbor route-server-client</code>	Configures this router as a route server and the specified neighbor as its client	RC
<code>neighbor send-community</code>	Configures the router to send community attributes to a neighbor in peering messages	RC
<code>neighbor shutdown</code>	Closes a neighbor connection without canceling the neighbor configuration	RC
<code>neighbor soft-reconfiguration inbound</code>	Configures the switch to store updates in the inbound message buffer, and perform soft re-configuration from this buffer for specified neighbors when required	RC
<code>neighbor strict-capability-match</code>	Forces strict capability matching when establishing connections	RC
<code>neighbor timers</code>	Sets the Keep Alive time and Hold time used for specified neighbors	RC
<code>neighbor timers connect</code>	Sets the time to wait before attempting to reconnect to a neighbor whose TCP connection has failed	RC
<code>neighbor unsuppress-map</code>	Allows specified suppressed routes to be advertised	RC
<code>neighbor update-source</code>	Specifies the interface to use for a connection, instead of using the nearest interface	RC
<code>neighbor weight</code>	Assigns a weight to a neighbor connection	RC
<i>Display Information</i>		
<code>show ip bgp</code>	Shows entries in the routing table	PE
<code>show ip bgp attribute-info</code>	Shows internal attribute information	PE
<code>show ip bgp cidr-only</code>	Shows routes which use classless inter-domain routing network masks	
<code>show ip bgp community</code>	Shows routes that belong to specified BGP communities	PE
<code>show ip bgp community-info</code>	Shows permitted community messages	PE
<code>show ip bgp community-list</code>	Shows the routes matching a community-list	PE
<code>show ip bgp dampening</code>	Shows dampened routes	PE
<code>show ip bgp filter-list</code>	Shows routes matching the specified filter list	PE
<code>show ip bgp neighbors</code>	Shows connection information for neighbor sessions	PE
<code>show ip bgp paths</code>	Shows all paths in the database	PE
<code>show ip bgp prefix-list</code>	Shows routes matching the specified prefix-list	PE
<code>show ip bgp regexp</code>	Shows routes matching the AS path regular expression	PE

Table 196: Border Gateway Protocol Commands – Version 4 (Continued)

Command	Function	Mode
show ip bgp route-map	Shows routes matching the specified route map	PE
show ip bgp scan	Shows BGP scan status	PE
show ip bgp summary	Shows summary information for all connections	PE
show ip community-list	Shows routes permitted by a community list	PE
show ip extcommunity-list	Shows routes permitted by an extended community list	PE
show ip prefix-list	Shows the specified prefix list	PE
show ip prefix-list detail	Shows detailed information for the specified prefix list	PE
show ip prefix-list summary	Shows summary information for the specified prefix list	PE

General Configuration

router bgp This command enables the Border Gateway Protocol (BGPv4) routing process and enters router configuration mode. Use the **no** form to disable it.

SYNTAX

[no] router bgp *as-number*

as-number – Autonomous system number which identifies this router as a member of the specified domain, and tags routing messages passed to other BGP routers with this number. (Range: 1-4294967295)

COMMAND MODE

Global Configuration

DEFAULT SETTING

No routing process is defined.

COMMAND USAGE

- ◆ To enable BGP routing, you must use this command to establish a BGP routing process. After entering this command, the switch enters router configuration mode.
- ◆ AS numbers in the range 64512-65535 are normally used for private routing domains, and can be removed from the AS path attribute in outbound routing messages using the [neighbor remove-private-as](#) command. Note that AS number 23456 is reserved for the AS-Transitive attribute which is required when setting up a new BGP speaker.
- ◆ Use this command to specify all of the routers within an autonomous system used to exchange interior or exterior BGP routing messages. Repeat this process for any other autonomous system under your administrative control to

create a distributed routing core for the exchange of routing information between autonomous systems.

EXAMPLE

```
Console(config)#router bgp 100
Console(config-router)#
```

RELATED COMMANDS

[network \(938\)](#)

ip as-path access-list This command configures an autonomous system path access list. Use the **no** form with only the access list name to disable its use, or with all parameters to remove a path attribute from the access list.

SYNTAX

ip as-path access-list *access-list-name* {**deny** | **permit**} *regular-expression*

no ip as-path access-list *access-list-name* [{**deny** | **permit**} *regular-expression*]

access-list-name – Name of the access list. (Maximum length: 16 characters, no spaces or other special characters)

deny – Permits access for messages with matching path attribute.

permit – Denies access to messages with matching path attribute.

regular-expression – Autonomous system in the access list expressed as a regular expression¹.

COMMAND MODE

Global Configuration

DEFAULT SETTING

No AS path access lists are defined.

COMMAND USAGE

- ◆ If the regular expression in an AS path list is matched, then the deny/permit condition is applied to the routing message.
- ◆ Use this command in conjunction with the [neighbor filter-list](#) command to filter route updates sent to or received from a neighbor, or with the [match as-path](#) route map command to implement a more comprehensive filter for policy-based routing.

1. Syntax complies with the IEEE POSIX Basic Regular Expressions (BRE) standard.

EXAMPLE

The regular expression in this example uses symbols which instruct the filter to match the character or null string at the beginning and end of an input string.

```
Console(config-router)#ip as-path access-list RD deny ^100$
Console(config-router)#
```

RELATED COMMANDS

[neighbor filter-list \(957\)](#)

[match as-path \(993\)](#)

ip community-list This command configures a community access list. Use the **no** form with only the access list name to disable its use, or with all parameters to remove a community attribute from the access list.

SYNTAX

[no] ip community-list

{1-99 | **standard** *community-list-name* {**deny** | **permit**}
[AA:NN] [**internet**] [**local-as**] [**no-advertise**] [**no-export**]} | {100-500 |
expanded *community-list-name* {**deny** | **permit**} *regular-expression*}

1-99 – Standard community list number that identifies one or more groups of communities.

standard *community-list-name* – Name of standard access list. A maximum of 16 communities can be configured in a standard community list (Maximum length: 32 characters, no spaces or other special characters)

deny – Denies access to messages with matching community attribute.

permit – Permits access for messages with matching community attribute.

AA:NN – Standard community-number to deny or permit. The 4-byte community number is composed of a 2-byte autonomous system number and a 2-byte network number, separated by one colon. Each 2-byte number can range from 0 to 65535. One or more communities can be entered, separated by a space. Up to 16 community numbers are supported.

internet – Specifies the entire Internet. Routes with this community attribute are advertised to all internal and external peers.

local-as – Specifies the local autonomous system. Routes with this community attribute are advertised only to peers that are part of the local autonomous system or to peers within a sub-autonomous system of a confederation. These routes are not advertised to external peers or to other sub-autonomous systems within a confederation.

no-advertise – Routes with this community attribute are not advertised to any internal or external peer.

no-export – Routes with this community attribute are advertised only to peers in the same autonomous system or to other sub-autonomous systems within a confederation. These routes are not advertised to external peers.

100-500 – Expanded community list number that identifies one or more groups of communities.

expanded *community-list-name* – Name of expanded access list.
(Maximum length: 32 characters, no spaces or other special characters)

regular-expression – Regular expression indicating the community list number or name¹.

COMMAND MODE

Global Configuration

DEFAULT SETTING

No community lists are defined.

COMMAND USAGE

- ◆ Standard community lists are used to configure well-known communities or community numbers. Expanded community lists are used to filter communities using a regular expression.
- ◆ When multiple values are entered in the same community list, they form a logical AND condition. When multiple values are configured in separate community lists, they form a logical OR condition, where the first list that matches a condition is processed.
- ◆ If the criteria specified for a community list is matched, then the deny/permit condition is applied to the routing message.
- ◆ If a permit value is applied to a community list, the filter will implicitly deny other community values.
- ◆ By default, the internet community is set with a route if no other communities are defined.
- ◆ Use this command in conjunction with the [neighbor send-community](#) to filter route updates sent to or received from a neighbor, or with the [match community](#) route map command to implement a more comprehensive filter for policy-based routing.

EXAMPLE

This example configures a named standard community list LN that permits routes with community value 100:10, denoting that they come from autonomous system 100 and network 10.

```
Console(config)#ip community-list standard LN permit 100:10
Console(config)#
```

RELATED COMMANDS

[neighbor send-community \(968\)](#)

[match community \(993\)](#)

ip extcommunity-list This command configures an extended community access list. Use the **no** form with only the access list name to disable its use, or with the relevant parameters to remove a community attribute from the access list.

SYNTAX

[no] ip extcommunity-list

```
{1-99 | standard community-list-name {deny | permit}
[{rt | soo} extended-community-value]} |
{100-500 | expanded community-list-name {deny | permit} regular-
expression}
```

1-99 – Standard community list number that identifies one or more groups of communities.

standard *community-list-name* – Name of standard access list. A maximum of 16 extended communities can be configured in a standard community list. (Maximum length: 32 characters, no spaces or other special characters)

deny – Denies access to messages with matching extended community attribute.

permit – Permits access for messages with matching extended community attribute.

rt – The route target extended community attribute.

soo – The site of origin extended community attribute.

extended-community-value – The route target or site of origin in one of the following formats:

AAAA:NN or *AA:NNNN* – Community-number to deny or permit. The community number can either be formatted as a 4-byte autonomous system number and a 2-byte network number, or as a 2-byte autonomous system number and a 4-byte network number, separated by one colon. Each 2-byte number can range from 0 to 65535, and 4-byte numbers from 0 to 4294967295.

IP:NN – Community to deny or permit. The community number is composed of a 4-byte IP address (representing the autonomous system

number) and a 2-byte network number, separated by one colon. The 2-byte network number can range from 0 to 65535.

One or more community numbers can be entered, separated by a space. Up to 3 community numbers are supported.

100-500 – Expanded community list number that identifies one or more groups of communities.

expanded *community-list-name* – Name of expanded access list.
(Maximum length: 32 characters, no spaces or other special characters)

regular-expression – Regular expression indicating the community list number or name. Syntax complies with the IEEE POSIX Basic Regular Expressions (BRE) standard.

COMMAND MODE

Global Configuration

DEFAULT SETTING

No extended community lists are defined.

COMMAND USAGE

- ◆ Standard community lists are used to configure well-known communities or community numbers. Expanded community lists are used to filter communities using a regular expression.
- ◆ When multiple values are entered in the same community list, they form a logical AND condition. When multiple values are configured in separate community lists, they form a logical OR condition, where the first list that matches a condition is processed.
- ◆ If the criteria specified for a community list is matched, then the deny/permit condition is applied to the routing message.
- ◆ If a permit value is applied to a community list, the filter will implicitly deny other community values.
- ◆ The route target (RT) attribute is used to identify sites that may receive routes tagged with a specific route target. Using this attribute allows that route to be placed in per-site forwarding tables used for routing traffic received from the corresponding sites.
- ◆ The site of origin (SOO) attribute is used to identify the site from which the provider edge (PE) router learned the route. All routes learned from a particular site are assigned the same site of origin attribute, no matter if a site is connected to a single PE router or multiple PE routers. Filtering based on this extended community attribute can prevent routing loops from occurring when a site is multi-homed.

- ◆ Use this command in conjunction with the [neighbor filter-list](#) to filter route updates sent to or received from a neighbor, or with the [match extcommunity](#) route map command to implement a more comprehensive filter for policy-based routing.

EXAMPLE

This example configures a named standard community list LR that permits routes with the route target 100:20, denoting that they destined for the autonomous system 100 and network 20.

```
Console(config)#ip extcommunity-list standard LP permit soo 100:20
Console(config)#
```

RELATED COMMANDS

[neighbor filter-list \(957\)](#)

[match extcommunity \(994\)](#)

ip prefix-list This command configures an IP address prefix list. Use the **no** form with only the prefix list name to disable its use, or with the relevant parameters to remove an attribute from the prefix list.

SYNTAX

```
[no] ip prefix-list prefix-list-name [seq sequence-number]
      {deny | permit} any
```

```
[no] ip prefix-list prefix-list-name [seq sequence-number]
      {deny | permit} {ip-address netmask | any}
      [ge min-prefix-length] [le max-prefix-length]
```

prefix-list-name – Name of prefix list. (Maximum length: 128 characters, no spaces or other special characters)

sequence-number – Applies a sequence number to the entry. If not specified, the entry is added to the bottom of the list, using a default numbering interval of 5. (Range: 1-429496725)

deny – Denies access to messages matching specified criteria.

permit – Permits access for messages matching specified criteria.

any – Any matching criteria.

ip-address – An IPv4 address expressed in dotted decimal notation.

netmask – Network mask for the route. This mask identifies the network address bits used for the associated routing entries.

ge – The minimum prefix length to match.

le – The maximum prefix length to match.

COMMAND MODE

Global Configuration

DEFAULT SETTING

No prefix lists are defined.

COMMAND USAGE

- ◆ Prefix filtering can be performed on an IP address expressed as a classful network, a subnet, or a single host route.
- ◆ Prefix lists are checked starting from the lowest sequence number and continues through the list until a match is found. Once an entry is found that covers a network, the permit or deny statement is applied to that network, and the search process stops.
- ◆ At least one “permit” statement should be included when more than one entry is defined. Commonly used “Deny” statements can be included at the top of the list to quickly remove unsuitable routing messages. If a list includes all “Deny” statements, then an entry of “permit 0.0.0.0 255.255.255.255 ge 0 le 32” can be included at the bottom of the list to grant passage for all other routing messages.
- ◆ A prefix list can be applied to inbound or outbound updates for a specific peer by entering the [neighbor prefix-list](#) command, or with the [match ip address prefix-list](#) route map command to implement a more comprehensive filter for policy-based routing.

EXAMPLE

This example denies access to routing messages for the specified address.

```
Console(config)#ip prefix-list LS deny 10.0.0.0 255.0.0.0 ge 14 le 22
Console(config)#
```

RELATED COMMANDS

[neighbor prefix-list \(963\)](#)

[match ip address \(995\)](#)

aggregate-address This command configures an aggregate address in the routing table. Use the **no** form to delete an aggregate address.

SYNTAX

[no] aggregate-address *ip-address netmask* [**as-set**] [**summary-only**]

ip-address – An IPv4 address expressed in dotted decimal notation.

netmask – Network mask for the route. This mask identifies the network address bits used for the associated routing entries.

as-set – Generates autonomous system set information for the AS path attribute, indicating that a route originated in multiple autonomous systems.

summary-only – Sends the summary routes only, ignoring more specific routes.

COMMAND MODE

Router Configuration

DEFAULT SETTING

No aggregate routes are defined.

COMMAND USAGE

- ◆ Using this command without any keywords will create an aggregate entry in the routing table if any more specific routes are available in the specified range. The aggregate route does not include any individual route attributes (e.g., AS-Path or Community). It is advertised as coming from this autonomous system and has the atomic aggregate attribute set to indicate that some information may be missing.
- ◆ Using the **as-set** keyword creates an aggregate route where the advertised path is an AS-Set that consists of all elements contained in all of paths being summarized. AS-Set information can be used to avoid routing loops because it records where the route has been. If a router notes its own AS number in the AS-Set of the aggregate update, it will drop the aggregate to prevent a loop. However, when aggregating tens or hundreds of routes, avoid advertising routing information in this manner, since this route may be frequently withdrawn and updated as AS path reachability information for the summarized routes changes.
- ◆ Using the **summary-only** keyword creates the aggregate route, while at the same time suppressing advertisements of more specific routes to all neighbors.

EXAMPLE

```
Console(config-router)#aggregate-address 100.1.0.0 255.255.0.0 summary-only
Console(config-router)#aggregate-address 100.2.0.0 255.255.0.0 summary-only
as-set
Console(config-router)#aggregate-address 100.3.0.0 255.255.0.0 as-set
Console(config-router)#end
Console#show ip bgp
BGP table version is 0, local router ID is 192.168.0.4
Status codes: s suppressed, d damped, h history, * valid, > best, i -
               internal,
                r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*>192.168.0.0/24	0.0.0.0	0		32768	i

bgp client-to-client reflection This command restores route reflection via this router. Use the **no** form to disable route reflection.

SYNTAX

[no] bgp client-to-client reflection

COMMAND MODE

Router Configuration

DEFAULT SETTING

Enabled

COMMAND USAGE

- ◆ Route reflection from this device is enabled by default, but is only functional if a client has been configured with the [neighbor route-reflector-client](#) command.
- ◆ Route reflection is not required if all of the routers in an AS are fully meshed as normally required by interior BGP. However, to make interior BGP more scalable, route reflection or confederations can be used. Route reflection uses one or more route reflectors to reflect routes between specified clients within a cluster. Clients within a reflector cluster therefore need not be fully meshed, and the exchange of routing information is thereby reduced since the clients need not communicate with any routers outside of the cluster.
- ◆ Routing information from an external BGP router is advertised to all cluster clients and non-client peers. Information from a non-client peer is advertised to all clients. And information from cluster members is reflected to all routing peers, both inside and outside of the cluster. using this model, the local AS can be divided into many clusters.
- ◆ Use the [bgp cluster-id](#) command to designate route reflectors within the same cluster so that route reflectors can recognize updates from other route reflectors in the same cluster.

EXAMPLE

```
Console(config-router)#bgp client-to-client reflection
Console(config-router)#
```

RELATED COMMANDS

[neighbor route-reflector-client \(966\)](#)
[bgp cluster-id \(931\)](#)

bgp cluster-id This command configures the cluster identifier for multiple route reflectors in the same cluster. Use the **no** form to remove the cluster identifier.

SYNTAX

bgp cluster-id *cluster-identifier*

no bgp cluster-id

cluster-identifier – The cluster identifier of this router when acting as a route reflector. This identifier can be expressed in the form an IPv4 address or an integer in the range of 1-4294967295.

COMMAND MODE

Router Configuration

DEFAULT SETTING

The router identifier of a lone route reflector in a cluster.

COMMAND USAGE

- ◆ A cluster of clients will usually have a single route reflector (RR). In that case, the cluster can be identified by the BGP Identifier of the RR. However, this represents a single point of failure. This command is used to designate multiple route reflectors used within the same cluster so that they can recognize updates from other peer route reflectors and discard them to prevent loopbacks.
- ◆ All the route reflectors in the same cluster should be fully meshed and all of them configured with identical sets of client and non-client peers.
- ◆ A route reflector uses the non-transitive cluster-list attribute to avoid routing loops. A cluster-list is a sequence of cluster IDs the route has passed through. When a RR reflects a route from its clients to non-client peers, and vice versa, it appends this ID to the cluster list. Using this attribute, an RR can determine if routing information has looped back to the same cluster due to mis-configuration. If the local cluster ID is found in the cluster list, the advertisement is ignored.

EXAMPLE

```
Console(config-router)#bgp cluster-id 192.168.0.0
Console(config-router)#
```

RELATED COMMANDS

[bgp client-to-client reflection \(930\)](#)

bgp confederation identifier This command configures the identifier for a confederation containing smaller multiple internal autonomous systems, and declares this router as a member of the confederation. Use the **no** form to remove the confederation identifier.

SYNTAX

bgp confederation identifier *as-number*

no bgp confederation identifier

as-number – Autonomous system number which identifies this router as a member of the specified domain, and tags routing messages passed to other BGP routers with this number. (Range: 1-4294967295)

COMMAND MODE

Router Configuration

DEFAULT SETTING

No confederation identifier is configured.

COMMAND USAGE

- ◆ BGP confederations are used to reduce the requirement for fully meshed connections between iBGP peers in the same AS. It works by dividing up a large AS into several smaller ASes, where only the peers in the same smaller AS are fully meshed, thus reducing the number of required connections and routing traffic.
- ◆ Even though different local confederation peers may have external BGP (eBGP) sessions, they exchange routing information among themselves as if they were iBGP peers. Next hop, Multi Exit Discriminator (MED), and local preference information is preserved. By preserving this information, a single Interior Gateway Protocol (IGP) can be used among the local confederations. When viewed from the outside by external peers, the larger AS is still identified as a single entity or autonomous system.
- ◆ Use the [bgp confederation peer](#) command to specify the autonomous systems within a confederation.

EXAMPLE

```
Console(config-router)#bgp confederation identifier 600
Console(config-router)#
```

RELATED COMMANDS

[bgp confederation peer \(933\)](#)

bgp confederation peer This command adds an internal peer autonomous system to a confederation. Use the **no** form to remove an autonomous system from a confederation.

SYNTAX

bgp confederation peer *as-number*

no bgp confederation identifier

as-number – Autonomous system number which identifies this router as a member of the specified domain, and tags routing messages passed to other BGP routers with this number. (Range: 1-4294967295)

COMMAND MODE

Router Configuration

DEFAULT SETTING

No confederation peer is configured.

COMMAND USAGE

- ◆ This command is used to add multiple ASes to a confederation. Each AS is fully meshed within itself, and the AS members are visible internally within the confederation.
- ◆ Use the [bgp confederation identifier](#) command to create a confederation.

EXAMPLE

This example divides AS 600 into four smaller ASes 101-104, and assigns a neighboring router as a member of the sub-AS 101.

```
Console(config-router)#bgp confederation identifier 600
Console(config-router)#bgp confederation peer 101
Console(config-router)#bgp confederation peer 102
Console(config-router)#bgp confederation peer 103
Console(config-router)#bgp confederation peer 104
Console(config-router)#neighbor 192.168.0.9 remote-as 101
Console(config-router)#
```

RELATED COMMANDS

[bgp confederation identifier \(932\)](#)

bgp dampening This command configures route dampening to reduce the propagation of unstable routes. Use the **no** form to restore the default settings.

SYNTAX

bgp dampening [*half-life* [*reuse-limit* [*suppress-limit* *max-suppress-time*]]]

no dampening

half-life – The time after which a penalty is reduced. The penalty value is reduced to half of the previous value after the half-life time expires.

(Range: 1-45 minutes)

reuse-limit – The point at which the penalty for a flapping route must fall before a route is unsuppressed. (Range: 1-2000)

suppress-limit – The point at which to start suppressing a route. (Range: 1-2000)

max-suppress-time – The maximum time a route can be suppressed. (Range: 1-255 minutes)

COMMAND MODE

Router Configuration

DEFAULT SETTING

half-life: 15 minutes

reuse-limit: 750

suppress-limit: 2000

max-suppress-time: 60 minutes (4 x half-life)

COMMAND USAGE

- ◆ Route dampening is used to reduce the frequency of routing updates due to unstable routes. Dampened routes are not used in the BGP decision process nor installed in the routing table.
- ◆ Each time a route flaps, the router assigns the route a penalty of 1000. If BGP receives an attribute change, BGP increases the penalty by 500. Penalties are cumulative, and the penalty for the route is stored in the BGP routing table until it exceeds the suppress limit. At that point, the route state changes to damped.
- ◆ Note that route dampening only applies to external BGP routes.

EXAMPLE

```
Console(config-router)#bgp dampening 20 1200 20000 220
Console(config-router)#
```

bgp enforce-first-as This command denies an update received from an external peer that does not list its own autonomous system number at the beginning of the AS path attribute. Use the **no** form to disable this feature.

SYNTAX

[no] bgp enforce-first-as

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

This command can be used to prevent a peer from misdirecting traffic by advertising a route as if sourced from another autonomous system.

EXAMPLE

```
Console(config-router)#bgp enforce-first-as
Console(config-router)#
```

bgp fast-external-failover This command resets sessions for any directly connected external peers if the link goes down. Use the **no** form to disable this feature.

SYNTAX

[no] bgp fast-external-failover

COMMAND MODE

Router Configuration

DEFAULT SETTING

Enabled

COMMAND USAGE

- ◆ This command immediately resets the connection for directly adjacent external peers if the interface goes down for any reason other than TCP timeout.
- ◆ If fast external failover is disabled, the routing process waits until the default hold timer expires to reset the session.

EXAMPLE

```
Console(config-router)#bgp fast-external-failover
Console(config-router)#
```

bgp log-neighbor-changes This command enables logging of neighbor resets (that is, up or down status changes). Use the **no** form to disable this feature.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

- ◆ This command helps detect network problems by indicating if a neighbor connection is flapping. A high number of neighbor resets might indicate unacceptable error rates or high packet loss in the network.
- ◆ Log messages for neighbor resets are recorded as level 6 messages in the system log file which can viewed using the [show log ram](#) command.

EXAMPLE

```
Console(config-router)#bgp log-neighbor-changes
Console(config-router)#
```

bgp network import-check This command checks for the existence of the next-hop and its accessibility to an Interior Gateway Protocol. Use the **no** form to disable this feature.

SYNTAX

[no] bgp network import-check

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

By default, BGP will advertise a route regardless of the Interior Gateway Protocol (IGP) in use. This command forces the router to verify the existence of the next hop for an advertised route, and to ensure that the route is accessible to an IGP.

EXAMPLE

```
Console(config-router)#bgp network import-check
Console(config-router)#
```


bgp router-id This command sets the router ID for this device. Use the **no** form to remove this ID.

SYNTAX

bgp router-id *router-id*

no bgp router-id

router-id – Router ID formatted as an IPv4 address.

COMMAND MODE

Router Configuration

DEFAULT SETTING

The highest IP address configured for an interface.

COMMAND USAGE

- ◆ By default, the router ID is automatically set to the highest IP address configured for a Layer 3 interface. This command can be used manually set the router ID to a fixed value.
- ◆ The router ID must be unique for every router in the autonomous system. Using the default setting based on the highest interface address ensures that each router ID is unique.
- ◆ All neighbor sessions will be reset if the router ID is changed.

EXAMPLE

```
Console(config-router)#bgp router-id 192.168.0.254
Console(config-router)#
```

bgp scan-time This command sets the interval at which to validate next hop information for BGP routes. Use the **no** form to restore the default setting.

SYNTAX

bgp scan-time *scan-time*

no bgp scan-time

scan-time – Next hop validation interval. (Range: 5-60 seconds)

COMMAND MODE

Router Configuration

DEFAULT SETTING

60 seconds

COMMAND USAGE

- ◆ This command sets the interval at which to check the validity of the next hop for all routes in the routing information database. During the interval between scan cycles, IGP instability or other network problems may cause black holes or routing loops to form.

EXAMPLE

```
Console(config-router)#bgp scan-time 30
Console(config-router)#
```

network This command specifies a network to advertise. Use the **no** form to stop advertising a network.

SYNTAX

network *ip-address* [*netmask*] [**route-map** *map-name* | [**backdoor**] **pathlimit** *ttl*]

no network *ip-address* [*netmask*]

ip-address – IP address of a to advertise.

netmask – Network mask for the route. This mask identifies the network address bits used for the associated routing entries.

map-name – Name of the route map. The route map can be used to filter the networks to advertise. (Range: 1-80 characters)

backdoor – Specifies a backdoor route to a BGP border router that provides better information about the network.

pathlimit *ttl* – Maximum number of hops allowed in an AS path. (Range: 0-255)

COMMAND MODE

Router Configuration

DEFAULT SETTING

No networks are configured.

COMMAND USAGE

- ◆ Use this command to specify the networks to advertise to BGP neighbors. BGP networks can be learned from directly connected routes, dynamic routing, or static route sources.
- ◆ BGP only sends and receives updates on interfaces specified by this command. If a network is not specified, the interfaces in that network will not be advertised in any BGP updates.
- ◆ A backdoor network has an administrative distance of 200, making routes learned through interior gateway protocols (RIP, OSPF, iBGP) preferred. A

backdoor network is treated as a local network, except that it not advertised by the local router. A backdoor route should not be sourced at the local router, but should be one that has been learned from external neighbors. However, since these routes are treated as a local network, they are given priority over routes learned through eBGP, even if the distance of the external route is shorter.

EXAMPLE

```
Console(config-router)#network 172.16.0.0 255.255.0.0
Console(config-router)#
```

redistribute This command redistributes routes from one routing domain to another. Use the **no** form to stop redistributing an previously configured entry.

SYNTAX

redistribute {**connected** | **ospf** | **rip** | **static**} [**metric** *metric-value*]
[**route-map** *map-name*]

no redistribute {**connected** | **ospf** | **rip** | **static**}
[**metric** *metric-value*] [**route-map** *map-name*]

connected - Imports routes that are established automatically just by enabling IP on an interface.

ospf - External routes will be imported from the Open Shortest Path First (OSPF) protocol into this routing domain.

ospf - External routes will be imported from the Routing Information Protocol (RIP) into this routing domain.

static - Static routes will be imported into this routing domain.

metric-value - Metric value assigned to all external routes for the specified protocol. (Range: 1-16)

map-name – Name of the route map. The route map can be used to filter the networks to advertise, and to modify their weight or other attributes. (Range: 1-80 characters)

COMMAND MODE

Router Configuration

DEFAULT SETTING

No redistribution is configured.

COMMAND USAGE

- ◆ Use this command to advertise routes that are learned by some other means, such as from another routing protocol or static routing entries. Since all internal routes are maintained by interior gateway protocols such as RIP and OSPF, careful filtering should be used to ensure that only routes that need to be advertised reach the Internet.

- ◆ A route metric must be used to resolve the problem of redistributing external routes with incompatible metrics.

EXAMPLE

```
Console(config-router)#redistribute static metric 10  
Console(config-router)#
```

timers bgp This command sets the Keep Alive time used for maintaining connectivity, and the Hold time to wait for Keep Alive or Update messages before declaring a neighbor down. Use the **no** form to restore the default settings.

SYNTAX

timers bgp *keepalive-time hold-time*

no timers bgp

keepalive-time – The frequency at which the local router sends keep-alive messages to its neighbors. (Range: 0-65535 seconds)

hold-time – The maximum interval after which a neighbor is declared dead if a keep-alive or update message has not been received. (Range: 0-65535 seconds)

COMMAND MODE

Router Configuration

DEFAULT SETTING

Keep Alive time: 60 seconds

Hold time: 180 seconds

COMMAND USAGE

- ◆ Use this command to set global BGP timers used for monitoring connectivity to neighboring routers. These timers will be applied to all neighbors unless the [neighbor timers](#) command has been used to explicitly configure other timer settings for a neighbor.
- ◆ When the minimum acceptable hold-time is configured with this command, a remote peer session can be established only if the neighboring router is advertising a hold-time equal to, or greater than, that configured on this device.

EXAMPLE

```
Console(config-router)#timers bgp 60 200  
Console(config-router)#
```

clear ip bgp This command clears connections using hard or soft re-configuration.

SYNTAX

```
clear ip bgp { * | as-number | external | peer-group group-name |  
neighbor-address } [in [prefix-list] | out | soft [in | out]]
```

***** – All BGP peering sessions.

as-number – All peering sessions within this autonomous system number.
(Range: 1-4294967295)

external – All eBGP peering sessions.

peer-group *group-name* – A BGP peer group containing a list of
neighboring routers configured with the [neighbor peer-group](#) command.

neighbor-address – IPv4 address of a neighbor.

in – Inbound sessions.

prefix-list – The outbound route filter (ORF) prefix list. This option triggers
a new route refresh or soft re-configuration, which updates the ORF prefix
list. This option is ignored unless ORF capabilities have been enabled using
the [neighbor capability orf prefix-list](#) command or ORF capability
information has been received from a sending peer. If ignored, a normal
inbound soft reset is performed.

out – Outbound sessions.

soft – Uses soft re-configuration for the reset, which does not tear down
the session.

COMMAND MODE

Privileged Exec

DEFAULT SETTING

None

COMMAND USAGE

- ◆ Use this command to initiate a hard reset or soft re-configuration. A hard reset
clears and rebuilds specified peering sessions and routing tables. Soft re-
configuration uses stored information to reconfigure and activate routing
tables without clearing existing sessions. It uses stored update information to
allow you to apply a new BGP policy without disrupting the network.
- ◆ To generate new inbound updates from stored information without resetting
peer sessions, you must preconfigure the local router using the [neighbor
capability orf prefix-list](#) command, which causes the router to store all received
updates. Note that storing updates is memory intensive and should only be
applied to critical links.

Outbound soft configuration requires no memory or preconfiguration. Outbound re-configuration can be used on the other side of a peering session to make initiate a new inbound policy on the local side.

- ◆ Use this command to clear peering sessions when changes are made to any BGP access lists, weights, or route-maps.
- ◆ Route refresh (RFC 2918) allows a router to reset inbound routing tables dynamically by exchanging route refresh requests with peers. Route refresh relies on the dynamic exchange of information with supporting peers. It is advertised through BGP capability negotiation, and all BGP routers must support this capability.

EXAMPLE

This example assumes that soft re-configuration has been set on the neighboring router.

```
Console(config-router)#clear ip bgp 192.168.0.254 soft in
Console(config-router)#
```

clear ip bgp dampening This command clears route dampening information and unsuppresses any currently suppressed routes.

SYNTAX

clear ip bgp dampening [*ip-address* [*netmask*]]

ip-address – IP address of network or peer router.

netmask – Network mask that identifies the network address bits.

COMMAND MODE

Privileged Exec

DEFAULT SETTING

None

EXAMPLE

If no keywords are entered as in this example, route dampening information is cleared for the entire routing table.

```
Console(config-router)#clear ip bgp dampening
Console(config-router)#
```

Route Metrics and Selection

bgp always-compare-med This command allows comparison of the Multi Exit Discriminator (MED) for paths advertised from neighbors in different autonomous systems. Use the **no** form to disable this feature.

SYNTAX

[no] bgp always-compare-med

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

- ◆ The MED is an optional non-transitive² attribute used to discriminate among multiple exit points to a neighboring autonomous system. A path with a lower MED is preferred over a path with a higher MED.
- ◆ By default, during best-path selection, the MED is compared only among paths from the same autonomous system. This command allows the comparison of MEDs among different paths regardless of the autonomous system from which the paths are received.
- ◆ The **bgp deterministic-med** command can be used to enforce comparison of the MED value between all paths received from within the same autonomous system.

EXAMPLE

This example assumes that a peer router is advertising the same route prefix through the two ASes (100 and 300) to the same AS (200), each of which carries a different MED.

```
Console(config-router)#bgp always-compare-med
Console(config-router)#
```

2. If a router does not understand an optional non-transitive attribute, it will be removed.

bgp bestpath as-path ignore This command ignores the AS path length in the selection of a path. Use the **no** form to disable this feature.

SYNTAX

[no] bgp bestpath as-path ignore

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

EXAMPLE

```
Console(config-router)#bgp bestpath as-path ignore
Console(config-router)#
```

**bgp bestpath compare-confed-
aspath** This command compare confederation AS path length in addition to external AS path length in the selection of a path. Use the **no** form to disable this feature.

SYNTAX

[no] bgp bestpath compare-confed-aspath

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

EXAMPLE

```
Console(config-router)#bgp bestpath compare-confed-aspath
Console(config-router)#
```

bgp bestpath compare-routerid This command compares similar routes from external peers, and gives preference to a route with the lowest router identifier. Use the **no** form to restore the default setting.

SYNTAX

[no] bgp bestpath compare-routerid

COMMAND MODE

Router Configuration

DEFAULT SETTING

When making the best-path selection, the router does not compare identical routes received from different external peers.

COMMAND USAGE

Normally, the first route arriving from different external peers (with other conditions equal) will be chosen as the best route. By using this command, the route with lowest router ID will be selected.

EXAMPLE

```
Console(config-router)#bgp bestpath compare-routerid
Console(config-router)#
```

bgp bestpath med This command enables comparison of the Multi Exit Discriminator (MED) attribute for paths learned from confederation peers, and the treatment of a route when the MED is missing. Use the **no** form to disable this feature.

SYNTAX

[no] bgp bestpath med {[confed] [missing-as-worst]}

confed – Compare MED in confederation path.

missing-as-worst – Consider as maximum MED value when missing.

COMMAND MODE

Router Configuration

DEFAULT SETTING

When making the best-path selection, the router does not consider the MED.

COMMAND USAGE

- ◆ The MED for paths learned from confederation peers is compared only if no external autonomous systems (AS) appear in the path. If an external AS is within the path, then the external MED is passed transparently through the confederation, and it is not compared.
- ◆ If the missing-as-worst option is disabled, the missing MED is assigned a value of 0, making a path missing the MED attribute the best path.

EXAMPLE

```
Console(config-router)#bgp bestpath med config missing-as-worst
Console(config-router)#
```

bgp default local-preference This command sets the default local preference used for best path selection among local iBGP peers. Use the **no** form to restore the default setting.

SYNTAX

bgp default local-preference *preference*

preference – Degree of preference iBGP peers give local routes during BGP best path selection. The higher the value, the more the route is to be preferred. (Range: 0-4294967295)

COMMAND MODE

Router Configuration

DEFAULT SETTING

100

COMMAND USAGE

Local preference is a discretionary attribute applied to a route during the BGP best path selection process. It is exchanged only between iBGP peers, and used to determine local policy.

EXAMPLE

```
Console(config-router)#bgp default local-preference 100
Console(config-router)#
```

bgp deterministic-med This command enforces deterministic comparison of the MED attribute between all paths received from the same AS, ensuring that selection of the best path will always be the same, regardless of the order in which the paths are received by the local router. Use the **no** form to disable this feature.

SYNTAX

[no] bgp deterministic-med

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

- ◆ The MED is compared after BGP attributes weight, local preference, AS-path and origin have been compared and are equal. When deterministic comparison of the MED is enabled, all paths for the same route prefix (received from peers within the same AS) are grouped together and arranged according to their MED value. Based on this comparison, the best path is then chosen.

- ◆ The router immediately groups and sorts all local paths when this command is entered. For correct results, deterministic comparison of the MED must be configured in the same manner (enabled or disabled) on all routers in the local AS.
- ◆ If deterministic comparison of the MED is not enabled, route selection can be affected by the order in which routes are received.
- ◆ This command compares the MED when choosing routes advertised by different peers in the same AS. To compare the MED when choosing routes from neighbors in different ASs, use the [bgp always-compare-med](#) command.

EXAMPLE

```
Console(config-router)#bgp deterministic-med
Console(config-router)#
```

distance This command sets the administrative distance for a specified external BGP (eBGP) routes. Use the **no** form to restore the default setting.

SYNTAX

distance *distance ip-address netmask [access-list-name]*

no distance *ip-address netmask*

distance – Administrative distance for an eBGP route. (Range: 1-255)

ip-address – IP address of a route entry.

netmask – Network mask for the route. This mask identifies the network address bits used for the associated routing entries.

access-list-name – Name of standard or extended access list.
(Maximum length: 16 characters, no spaces or other special characters)

COMMAND MODE

Router Configuration

DEFAULT SETTING

None

COMMAND USAGE

- ◆ The route distance indicates the trustworthiness of a router. The higher the distance the lower the trust rating. A distance of 255 means that the routing source cannot be trusted and should be ignored.
- ◆ This distance set by this command only applies to external BGP paths routes learned from a neighbor outside of the AS. Use the [distance bgp](#) command to configure the global setting for the distance of eBGP, iBGP, and local routes.

- ◆ If an access-list is specified, it will be applied to received routes. If the received routes are not matched in the access-list or the specified list does not exist, the original distance value will be used.

EXAMPLE

```
Console(config-router)#distance 90 10.1.1.64 255.255.255.255  
Console(config-router)#
```

RELATED COMMANDS

[distance bgp \(948\)](#)

distance bgp This command sets the administrative distance for external BGP, internal BGP, and local routes. Use the **no** form to restore the default settings.

SYNTAX

distance bgp *ebgp-distance ibgp-distance local-distance*

no distance bgp

ebgp-distance – Administrative distance for eBGP routes. (Range: 1-255)

ibgp-distance – Administrative distance for iBGP routes. (Range: 1-255)

local-distance – Administrative distance for local routes. (Range: 1-255)

COMMAND MODE

Router Configuration

DEFAULT SETTING

eBGP: 20

iBGP: 200

local: 200

COMMAND USAGE

- ◆ External routes are learned from an external autonomous system, and internal routes from a peer within the local autonomous system. Local routes are those configured with the [network](#) command as a back door for the router or for the networks being redistributed from another routing process.
- ◆ The route distance indicates the trustworthiness of a router. The higher the distance the lower the trust rating. A distance of 255 means that the routing source cannot be trusted and should be ignored.
- ◆ This command can be used to indicate that another protocol can provide a better route to a node than that learned via eBGP, or to indicate that some internal routes should be preferred by BGP.

- ◆ Changing the administrative distance of iBGP routes is not recommended. It may cause an accumulation of routing table inconsistencies which can break routing to many parts of the network.

EXAMPLE

```
Console(config-router)#distance bgp 20 200 20
Console(config-router)#
```

RELATED COMMANDS

[distance \(947\)](#)

Neighbor Configuration

neighbor activate This command enables the exchange of routing information with a neighboring router or peer group. Use the **no** form to disable the exchange of routing information.

SYNTAX

[no] neighbor {ip-address | group-name} activate

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the [neighbor peer-group](#) command.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Enabled

COMMAND USAGE

- ◆ After a connection is opened with a neighboring router, this command is used to enable the exchange of information with the neighbor.
- ◆ The exchange of information is enabled by default for each routing session configured with the [neighbor remote-as](#) command.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 activate
Console(config-router)#
```

neighbor advertisement-interval This command configures the interval between sending update messages to a neighbor. Use the **no** form to restore the default setting.

SYNTAX

neighbor *ip-address* **advertisement-interval** *interval*

no neighbor *ip-address* **advertisement-interval**

ip-address – IP address of a neighbor.

interval – The minimum interval between sending routing updates to the specified neighbor. (Range: 0-600 seconds)

COMMAND MODE

Router Configuration

DEFAULT SETTING

iBGP: 5 seconds

eBGP: 30 seconds

COMMAND USAGE

This command can be used to reduce route flapping. However, the [bgp dampening](#) command can provide more precise control of route flapping.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 advertisement-interval 20
Console(config-router)#
```

neighbor allowas-in This command configures the number of times the AS path for a received route can contain the same AS number. Use the **no** form to restore the default setting.

SYNTAX

neighbor {*ip-address* | *group-name*} **allowas-in** [*count*]

no neighbor {*ip-address* | *group-name*} **allowas-in**

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the [neighbor peer-group](#) command.

count – Maximum number of times the same AS number can appear in the AS path of a received route. (Range: 1-10, or 3 if the count is not undefined)

COMMAND MODE

Router Configuration

DEFAULT SETTING

No repeats allowed

COMMAND USAGE

Under standard routing practices, BGP will not accept a route sent from a neighbor if the same AS number appears in the AS path more than once. This could indicate a routing loop, and the route message would therefore be dropped. However, for purposes of traffic engineering (such as degrading the preference for a certain path), this command can be used to configure the number of times the same AS is allowed re-appear in the AS path of a route received from a neighbor.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 allowas-in 5
Console(config-router)#
```

neighbor attribute- unchanged

This command configures certain route attributes to be kept unchanged for transparent transmission to the specified neighbor. Use the **no** form to disable this feature.

SYNTAX

**[no] neighbor {ip-address | group-name} attribute-unchanged [as-path]
[med] [next-hop]**

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the [neighbor peer-group](#) command.

as-path – AS path attribute

med – Mult-Exit Discriminator (MED) attribute

next-hop – Next hop attribute

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

If this command is entered without specifying any route attributes, then all three optional attributes are used.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 attribute-unchanged
Console(config-router)#
```

neighbor capability dynamic This command configures dynamic negotiation of capabilities between neighboring routers. Use the **no** form to disable this feature.

SYNTAX

[no] neighbor {ip-address | group-name} capability dynamic

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the [neighbor peer-group](#) command.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

- ◆ BGP normally requires a router to terminate a peering session if it receives an OPEN message with an unrecognized optional parameter. This command allows new capabilities to be introduced gracefully, without requiring a peering session to be terminated if a negotiated capability is unknown.
- ◆ With dynamic negotiation of capabilities is enabled, the capabilities by both sides are negotiated in OPEN messages, with the partner responding if a capability is supported or sending a NOTIFICATION if not.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 capability dynamic
Console(config-router)#
```

neighbor capability orf prefix-list This command configures the negotiation of outbound route filter (ORF) capabilities with a neighboring router. Use the **no** form to disable negotiation.

SYNTAX

[no] neighbor {ip-address | group-name} orf prefix-list {both | receive | send}

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the [neighbor peer-group](#) command.

both – Capability to send and receive the ORF to/from this neighbor.

receive – Capability to receive the ORF from this neighbor.

send – Capability to send the ORF to this neighbor.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

When this command is entered, the side configured with inbound prefix-list filter rules will transmit its own rules to the peer, and the peer will then use these rules as its own outbound rules, thereby avoiding sending routes which will be denied by its partner.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 orf prefix-list both
Console(config-router)#
```

neighbor default-originate This command allows the local router to send a default route to a neighbor. Use the **no** form to disable this feature.

SYNTAX

neighbor {*ip-address* | *group-name*} **default-originate** [**route-map** *map-name*]

no neighbor {*ip-address* | *group-name*} **default-originate**

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the [neighbor peer-group](#) command.

map-name – Name of the route map. The route map can be used to filter the criteria used for sending the default route to a neighbor. (Range: 1-80 characters)

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

- ◆ This command is used to advertise the local router's default route (0.0.0.0) to a neighbor. This route can be used by the neighbor to reach the local router if no other routes are available.
- ◆ If several neighbors supply a default route to the same partner, the best one will be elected according to the standard path selection process.

- ◆ If a route map is specified, the default route 0.0.0.0 is advertised if the route map contains a **match ip address** clause and there is a route that matches an entry in the **ip prefix-list**.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 default-originate
Console(config-router)#
```

neighbor description This command configures the description of a neighbor or peer group. Use the **no** form to remove a description.

SYNTAX

neighbor {*ip-address* | *group-name*} **description** *description*

no neighbor {*ip-address* | *group-name*} **description**

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the **neighbor peer-group** command.

description – Descriptive string. (Range: 1-80 characters)

COMMAND MODE

Router Configuration

DEFAULT SETTING

No description specified

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 description bill's router
Console(config-router)#
```

neighbor distribute-list This command filters route updates to/from a neighbor or peer group. Use the **no** form to remove this list.

SYNTAX

neighbor {*ip-address* | *group-name*} **distribute-list** *access-list-name* {**in** | **out**}

no neighbor {*ip-address* | *group-name*} **distribute-list** {**in** | **out**}

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the **neighbor peer-group** command.

access-list-name – Name of standard or extended access list.
(Maximum length: 32 characters, no spaces or other special characters)

in – Filters inbound routing messages.

out – Filters outbound routing messages.

COMMAND MODE

Router Configuration

DEFAULT SETTING

None

COMMAND USAGE

- ◆ If the specified access list for input or output mode does not exist, all input or output route updates will be filtered.
- ◆ The [neighbor prefix-list](#) and the neighbor distribute-list commands are mutually exclusive for a BGP peer. That is, only one of these commands may be applied in the inbound or outbound direction.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 distribute-list RD in
Console(config-router)#
```

neighbor dont-capability-negotiate This command disables capability negotiation when creating connections. Use the **no** form to restore the default setting.

SYNTAX

[no] neighbor {ip-address | group-name} dont-capability-negotiate

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the [neighbor peer-group](#) command.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Capability negotiation is enabled

COMMAND USAGE

Earlier versions of BGPv4 require that when a BGP speaker receives an Open message with one or more unrecognized Optional Parameters, the speaker must terminate BGP peering. This command can be used when connecting to a partner known to use an older BGP version which does not support capabilities negotiation (RFC 2842), thereby allowing the peering session to continue.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 dont-capability-negotiate
Console(config-router)#
```

neighbor ebgp-multihop This command allows eBGP neighbors to exist in different segments, and configures the maximum hop count (TTL). Use the **no** form to restore the default setting.

SYNTAX

neighbor {*ip-address* | *group-name*} **ebgp-multihop** [*count*]

no neighbor {*ip-address* | *group-name*} **ebgp-multihop**

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the [neighbor peer-group](#) command.

count – Maximum hop count. (Range: 1-255)

COMMAND MODE

Router Configuration

DEFAULT SETTING

eBGP neighbors must be located in the same segment.

COMMAND USAGE

- ◆ This command can be used to allow routers in different network segments to create a BGP neighbor relationship.
- ◆ If this command is entered without specifying a count, the hop limit is set at 255.
- ◆ To avoid creating loops through oscillating routes, a multi-hop session will not be established if the only route to a multi-hop peer is the default route.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 ebgp-multihop 2
Console(config-router)#
```

neighbor enforce-multihop This command enforces the requirement for all neighbors to form multi-hop connections. Use the **no** form to disable this requirement.

SYNTAX

[no] neighbor {ip-address | group-name} enforce-multihop

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the [neighbor peer-group](#) command.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Not enforced

COMMAND USAGE

By default, the multi-hop check is only performed on iBGP and eBGP non-direct routes. This command can be used to force the router to perform the multi-hop check on directly connected routes as well. In other words, the router will not perform the next-hop direct-connect check the specified neighbor.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 enforce-multihop
Console(config-router)#
```

neighbor filter-list This command filters route updates sent to or received from a neighbor based on an AS path access-list. Use the **no** form to disable route filtering.

SYNTAX

neighbor {ip-address | group-name} filter-list access-list {in | out}

no neighbor {ip-address | group-name} filter-list {in | out}

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the [neighbor peer-group](#) command.

access-list – Name of an AS-Path access list configured with the [ip as-path access-list](#) command.

in – Filter inbound routing updates.

out – Filter outbound routing updates.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

Use this command in conjunction with the [ip as-path access-list](#) command to filter route updates sent to or received from a neighbor.

EXAMPLE

In this example, the AS path access list “ASPF” is first configured to deny access to any route passing through AS 100. It then enables route filtering by assigning this list to a peer.

```
Console(config)#ip as-path access-list ASPF deny 100
Console(config)#router bgp 100
Console(config-router)#redistribute static
Console(config-router)#neighbor 10.1.1.66 filter-list ASPF out
Console(config-router)#
```

neighbor interface This command specifies the interface to a neighbor. Use the **no** form to remove this configuration setting.

SYNTAX

neighbor *ip-address* interface **vlan *vlan-id***

no neighbor *ip-address* interface

ip-address – IP address of a neighbor.

vlan-id - VLAN ID. (Range: 1-4094)

COMMAND MODE

Router Configuration

DEFAULT SETTING

None

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 interface vlan 1
Console(config-router)#
```

neighbor maximum-prefix This command sets the maximum number or route prefixes that can be received from a neighbor. Use the **no** form to restore the default setting.

SYNTAX

neighbor {*ip-address* | *group-name*} **maximum-prefix** *max-count* [*threshold* [**restart** *interval* | **warning**]]

no neighbor {*ip-address* | *group-name*} **maximum-prefix**

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the [neighbor peer-group](#) command.

max-count – The maximum number of route prefixes that will be accepted from a neighbor. (Range: 1-4294967295)

threshold – The percentage of the maximum number of allowed prefixes at which the router will initiate the specified response.

restart – Restarts BGP connection after the threshold is exceeded.

interval – Time to wait after a BGP connection has been terminated, before reestablishing the session. (Range: 1-65535 minutes)

warning – Sends a log message if the threshold is exceeded.

COMMAND MODE

Router Configuration

DEFAULT SETTING

No limit is set

DEFAULT USAGE

- ◆ This command is used to control the maximum number of route prefixes that can be sent by a neighbor. It provides a method to reserve resources for other processes, or to prevent malicious attacks.
- ◆ If the threshold is specified, but neither the **restart** nor **warning** keywords are used), the connection will be closed until the records are cleared with the [clear ip bgp](#) command.

EXAMPLE

In this example, the router warns when the number of route prefixes reaches 6, and the connection will be closed when the prefixes hit 13.

```
Console(config-router)#neighbor 10.1.1.64 maximum-prefix 12 50
Console(config-router)#
```

neighbor next-hop-self This command configures the local router as the next hop for a neighbor in all routing messages it sends. Use the **no** form to disable this feature.

SYNTAX

[no] neighbor {ip-address | group-name} next-hop-self

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the [neighbor peer-group](#) command.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

DEFAULT USAGE

- ◆ iBGP routers only connected to other iBGP routers in same segment will not be able to talk with iBGP routers outside of the segment if they are not directly connected with each other. This command can be used in these kinds of networks (i.e., un-meshed or non-broadcast) where iBGP neighbors may not have direct access to all other neighbors on the same IP subnet.
- ◆ Even when a successful BGP relationship seems to have been established within the local AS, you may not be able to see some routes in the routing table. iBGP routers only connected with other iBGP routers in same AS will not be able to talk with routers outside of the AS if they are not directly connected with each other. The **neighbor next-hop-self** command can be used to configure an iBGP router which is directly connected with an eBGP neighbor so that other iBGP routers in the same AS can talk with eBGP routers outside the AS.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 next-hop-self
Console(config-router)#
```

neighbor override-capability This command overrides the result of capability negotiations, allowing a session to be formed with a peer that does not support capability negotiation. Use the **no** form to disable this feature.

SYNTAX

[no] neighbor {ip-address | group-name} neighbor override-capability

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the [neighbor peer-group](#) command.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 override-capability
Console(config-router)#
```

neighbor passive This command passively forms a connection with the specified neighbor, not sending a TCP connection request, but waiting a connection request from the specified neighbor. Use the **no** form to disable this feature.

SYNTAX

[no] neighbor {ip-address | group-name} passive

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the [neighbor peer-group](#) command.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

This command configures the local router so that it remains in Active state, waiting for an inbound connection request from a neighbor, and not initiating any outbound connections with the neighbor via an Open message.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 passive
Console(config-router)#
```

neighbor peer-group (Creating) This command configures a router peer group which can be easily configured with the same attributes. Use the **no** form to remove a peer group.

SYNTAX

[no] neighbor group-name peer-group

group-name – A BGP peer group. (Range: 1-256 characters)

COMMAND MODE

Router Configuration

DEFAULT SETTING

No peer groups are defined.

COMMAND USAGE

- ◆ Neighbors with the same BGP attributes can be grouped into peer groups. This simplifies the application of various policies, such as filter lists. Other configuration settings can be applied to a peer-group using any of the neighbor commands. Any changes made to the peer group affect all members. Use this command to create a peer-group.
- ◆ To assign members to a peer group, use the [neighbor ip-address peer-group group-name](#) command.

EXAMPLE

```
Console(config-router)#neighbor RD peer-group  
Console(config-router)#
```

neighbor peer-group (Group Members) This command assigns routers to a peer group. Use the **no** form to remove a group member.

SYNTAX

[no] neighbor ip-address peer-group group-name

ip-address – IP address of a neighbor.

group-name – A BGP peer group.

COMMAND MODE

Router Configuration

DEFAULT SETTING

No group members are defined.

COMMAND USAGE

To create a peer group, use the [neighbor group-name peer-group](#) command.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 peer-group RD  
Console(config-router)#
```

neighbor port This command specifies the TCP port number of the partner through which communications are carried. Use the **no** form to restore the default setting.

SYNTAX

neighbor *ip-address* **port** *port-number*

no neighbor *ip-address* **port**

ip-address – IP address of a neighbor.

port-number – TCP port number to use for BGP communications.
(Range: 0-65535)

COMMAND MODE

Router Configuration

DEFAULT SETTING

179

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 port 1023
Console(config-router)#
```

neighbor prefix-list This command configures prefix restrictions applied in inbound/outbound route updates to/from specified neighbors. Use the **no** form to remove the neighbor binding for a prefix list.

SYNTAX

neighbor {*ip-address* | *group-name*} **prefix-list** *list-name* {**in** | **out**}

no neighbor {*ip-address* | *group-name*} **prefix-list** {**in** | **out**}

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the [neighbor peer-group](#) command.

list-name – Name of a prefix-list. The prefix list can be used to filter the networks to import or export. (Range: 1-80 characters)

in – Filter inbound routing updates.

out – Filter outbound routing updates.

COMMAND MODE

Router Configuration

DEFAULT SETTING

No prefix list restrictions are configured.

COMMAND USAGE

- ◆ First, configure a prefix list with the `ip prefix-list` command, and then use this command to specify the neighbors to which it applies, and whether it applies to inbound or outbound messages.
- ◆ Filtering routes based on a prefix list searches for entries matching the router specified by this command. If a match is found and the entry is configured to permit the route, the route will be imported or exported as defined by this command. An empty prefix list permits all prefixes. If a prefix does not match any entries in a list, the route is denied. When multiple entries in the list match a prefix, the entry with the smallest sequence number is used.
- ◆ The search starts at the top of the prefix list. Once an entry matches, the router stops searching. To reduce the load on system resources, the most commonly used entries should be placed at the top of the list.

EXAMPLE

```
Console(config)#ip prefix-list RD permit 100.1.0.0 255.255.0.0 ge 17 le 18
Console(config)#router bgp 200
Console(config-router)#redistribute static
Console(config-router)#neighbor 10.1.1.66 prefix-list RD out
Console(config-router)#
```

neighbor remote-as This command configures a neighbor and its AS number, identifying the neighbor as an iBGP or eBGP peer. Use the **no** form to remove a neighbor.

SYNTAX

neighbor {*ip-address* | *group-name*} **remote-as** *as-number*

no neighbor {*ip-address* | *group-name*} **remote-as**

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the `neighbor peer-group` command.

as-number – Autonomous system number which identifies this router as a member of the specified domain, and tags routing messages passed to other BGP routers with this number. (Range: 1-4294967295)

COMMAND MODE

Router Configuration

DEFAULT SETTING

No neighbors are configured.

COMMAND USAGE

- ◆ BGP neighbors must be manually configured. A neighbor relationship can only be established if partners are configured on both sides a connection.

- ◆ If the neighbor's AS number is the same as that of the local router, the neighbor is an iBGP peer. If it is different, the neighbor is an eBGP peer.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 remote-as 100
Console(config-router)#
```

neighbor remove-private-as This command removes private autonomous system numbers from outbound routing updates to an external neighbor. Use the **no** form to disable this feature.

SYNTAX

neighbor {*ip-address* | *group-name*} **remove-private-as**

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the [neighbor peer-group](#) command.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

- ◆ This command only applies to eBGP neighbors. It is used to avoid passing an internal AS number to an external AS. Internal AS numbers range from 64512-65535, and should not be sent to the Internet since they are not valid external AS numbers.
- ◆ This configuration only takes effect when the AS Path attribute of a route contains only internal AS numbers. If the AS Path attribute for a route contains both internal and external AS numbers, the route will not be processed.
- ◆ This command may be used in BGP confederations provided that the private AS numbers appear after the confederation portion of the AS path.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 remove-private-as
Console(config-router)#
```

neighbor route-map This command specifies the route mapping policy for inbound/outbound routing updates for specified neighbors. Use the **no** form to remove this policy binding.

SYNTAX

neighbor {*ip-address* | *group-name*} **route-map** *map-name* {**in** | **out**}

no neighbor {*ip-address* | *group-name*} **route-map** {**in** | **out**}

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the [neighbor peer-group](#) command.

map-name – Name of the route map. The route map can be used to filter the networks to advertise or receive based on various attributes.
(Range: 1-128 characters)

in – Filter inbound routing updates.

out – Filter outbound routing updates.

COMMAND MODE

Router Configuration

DEFAULT SETTING

No route maps are configured nor bound to any neighbor.

COMMAND USAGE

- ◆ First, use [route-map](#) command to create a route map, and the **match** and **set** commands to configure the route attributes to act upon. Then use this command to specify neighbors to which the route map is applied.
- ◆ If the specified route map does not exist, all input/output route updates will be filtered.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 route-map RD in
Console(config-router)#
```

neighbor route-reflector-client This command configures this router as a route reflector and the specified neighbor as its client. Use the **no** form to disable route reflection for the specified neighbor.

SYNTAX

[**no**] **neighbor** {*ip-address* | *group-name*} **route-reflector-client**

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the [neighbor peer-group](#) command.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

- ◆ Route reflection from this device is enabled by default, but is only functional if a client has been configured with this command.
- ◆ Under standard configuration rules, all BGP speakers within the same AS must be fully meshed. Route reflection can be used to reduce the number of connections required between peers. Reflector clients exchange messages only with the route reflector, while the reflector handles message exchanges among each client and other iBGP, eBGP, and non-client routers. For more information on configuring route reflection, refer to the Command Usage section under the [bgp client-to-client reflection](#) command.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 route-reflector-client
Console(config-router)#
```

neighbor route-server-client This command configures this router as a route server and the specified neighbor as its client. Use the **no** form to disable the route server for the specified neighbor.

SYNTAX

[no] neighbor {ip-address | group-name} route-server-client

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the [neighbor peer-group](#) command.

COMMAND MODE

Router Configuration

DEFAULT SETTING

None

COMMAND USAGE

- ◆ A route server is used as a replacement for full mesh eBGP routing in internet exchange points in a manner similar to the way route reflectors are used in iBGP. Instead of maintaining direct eBGP peering sessions with every other service provider, providers can acquire the same routing information through a single connection to a route server at the Internet exchange.

- ◆ Using a route server reduces the configuration complexity required for an eBGP full mesh, limits CPU and memory requirements for the exchange of peering messages, and avoids the need for negotiating a large number of individual peering agreements.

EXAMPLE

In the following example, the router 10.1.1.64 (AS100) is configured as the route server for neighbors 10.1.1.66 (AS200) and 10.1.1.68 (AS300).

```
Console(config)#router bgp 100
Console(config-router)#neighbor 10.1.1.66 remote-as 200
Console(config-router)#neighbor 10.1.1.66 route-server-client
Console(config-router)#neighbor 10.1.1.68 remote-as 300
Console(config-router)#neighbor 10.1.1.68 route-server-client
Console(config-router)#
```

neighbor send-community This command configures the router to send community attributes to a neighbor in peering messages. Use the **no** form to stop sending this attribute to a neighbor.

SYNTAX

[no] neighbor {ip-address | group-name} send-community
[both | extended | standard]

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the [neighbor peer-group](#) command.

both – Sends both extended and standard community attributes.

extended – Sends extended community attributes.

standard – Standard community attributes.

COMMAND MODE

Router Configuration

DEFAULT SETTING

No community attributes are sent. If community type is not specified, then only standard community attributes are sent.

COMMAND USAGE

Community attributes are used to group destinations into a certain community, and apply routing decisions to the overall community.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.66 send-community extended
Console(config-router)#
```


RELATED COMMANDS

[set community \(1002\)](#)

neighbor shutdown This command closes a neighbor connection without canceling the neighbor configuration. Use the **no** form to restore the connection.

SYNTAX

[no] neighbor {ip-address | group-name} shutdown

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the [neighbor peer-group](#) command.

COMMAND MODE

Router Configuration

DEFAULT SETTING

None

COMMAND USAGE

- ◆ This command terminates any active sessions for the specified neighbor, and removes any associated routing information.
- ◆ Use the [show ip bgp summary](#) command display the neighbors which have been administratively shut down. Entries with in an Idle (Admin) state have been disabled by the **neighbor shutdown** command.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.66 shutdown
Console(config-router)#
```

neighbor soft-reconfiguration inbound This command configures the switch to store updates in the inbound message buffer, and perform soft re-configuration from this buffer for specified neighbors when required. Use the **no** form to disable this feature.

SYNTAX

[no] neighbor {ip-address | group-name} soft-reconfiguration inbound

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the [neighbor peer-group](#) command.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

- ◆ Use this command to employ soft reconfiguration for a neighbor. A hard reset clears and rebuilds specified peering sessions and routing tables. Soft reconfiguration uses stored information to reconfigure and activate routing tables without clearing existing sessions. It uses stored update information to allow you to restore a connection or to apply a new BGP policy without disrupting the network. Note that outbound soft reconfiguration does not require inbound soft reconfiguration to be enabled.
- ◆ The command is only available when route refresh capability is not enabled. Route refresh (RFC 2918) allows a router to reset inbound routing tables dynamically by exchanging route refresh requests with peers. Route refresh relies on the dynamic exchange of information with supporting peers. It is advertised through BGP capability negotiation, and all BGP routers must support this capability.
- ◆ To use soft reconfiguration, without preconfiguration, both BGP neighbors must support the soft route refresh capability advertised in open messages sent when a BGP session is established. To see if a BGP router supports this capability, use the [show ip bgp neighbors](#) command.

EXAMPLE

```
Console(config-router)#neighbor 11.1.1.120 soft-reconfiguration inbound  
Console(config-router)#
```

neighbor strict-capability-match This command forces strict capability matching when establishing connections. Use the **no** form to disable this requirement.

SYNTAX

[no] neighbor {ip-address | group-name} strict-capability-match

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the [neighbor peer-group](#) command.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

This command specifies that a connection can only be established when the both sides have perfectly matching capabilities.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.66 strict-capability-match
Console(config-router)#
```

neighbor timers This command sets the Keep Alive time and Hold time used for specified neighbors. Use the **no** form to restore the default settings.

SYNTAX

[no] neighbor {ip-address | group-name} timers keepalive-time hold-time

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the [neighbor peer-group](#) command.

keepalive-time – The frequency at which the local router sends keep-alive messages to its neighbors. (Range: 0-65535 seconds)

hold-time – The maximum interval after which a neighbor is declared dead if a keep-alive or update message has not been received. (Range: 0-65535 seconds)

COMMAND MODE

Router Configuration

DEFAULT SETTING

Keep Alive time: 60 seconds

Hold time: 180 seconds

COMMAND USAGE

- ◆ This command sets the Keep Alive time used for maintaining connectivity, and the Hold time to wait for Keep Alive or Update messages before declaring a neighbor down.
- ◆ This command sets timers for monitoring connectivity to specific neighboring routers, which supercede those applied to all neighbors with the global [timers bgp](#) command.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.66 timers 50 200
Console(config-router)#
```

neighbor timers connect This command sets the time to wait before attempting to reconnect to a neighbor whose TCP connection has failed. Use the **no** form to restore the default setting.

SYNTAX

[no] neighbor ip-address timers connect retry-interval

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the [neighbor peer-group](#) command.

retry-interval – The amount of time the system waits for the transport protocol connection to complete. If this timer expires, the state remains in Connect state, the timer is reset, and the system tries to initiate a new transport connection. (Range: 0-65535 seconds)

COMMAND MODE

Router Configuration

DEFAULT SETTING

120 seconds

COMMAND USAGE

This command sets the time to wait before attempting to reconnect to a BGP neighbor after having failed to connect. During the idle time specified by the Connect Retry timer, the remote BGP peer can actively establish a BGP session with the local router.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.66 timers connect 100
Console(config-router)#
```

neighbor unsuppress-map This command allows routes suppressed by the [aggregate-address](#) (summary-only option) to be advertised to specified neighbors. Use the **no** form to remove this configuration entry.

SYNTAX

[no] neighbor {ip-address | group-name} unsuppress-map map-name

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the [neighbor peer-group](#) command.

map-name – Name of the route map. The route map can be used to filter the networks to advertise. (Range: 1-80 characters)

COMMAND MODE

Router Configuration

DEFAULT SETTING

No exceptions

COMMAND USAGE

This command is used to leak routes suppressed by the [aggregate-address](#) command (with summary-only option) to specified neighbors. Other routes that meet the route map conditions, but have not been suppressed, will still be sent.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.66 unsuppress-map rmp
Console(config-router)#
```

neighbor update-source

This command specifies the interface to use for a TCP connection, instead of using the nearest interface. Use the **no** form to use the default interface.

SYNTAX

[no] neighbor {ip-address | group-name} update-source interface vlan vlan-id

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the [neighbor peer-group](#) command.

vlan-id - VLAN ID. (Range: 1-4094)

COMMAND MODE

Router Configuration

DEFAULT SETTING

The nearest (best/closest) interface is used.

COMMAND USAGE

By default the nearest interface to the neighbor is used for BGP connections. This command can be used to specify any available interface for a TCP connection.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.66 update-source interface vlan 1
Console(config-router)#
```

neighbor weight This command assigns a weight to routes sent from a neighbor. Use the **no** form to restore the default weight.

SYNTAX

neighbor {*ip-address* | *group-name*} **weight** *weight*

no neighbor {*ip-address* | *group-name*} **weight**

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the [neighbor peer-group](#) command.

weight – The weight to be assigned to routes received from this neighbor. (Range: 0-65535)

COMMAND MODE

Router Configuration

DEFAULT SETTING

Routes learned from a neighbor: 0

Static routes sourced by the local router: 32768

COMMAND USAGE

- ◆ Use this command to specify a weight for all the routes learned from a neighbor. The route with the highest weight gets preference over other routes to the same network.
- ◆ Weights assigned using the [set weight](#) command override those assigned by this command.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.66 weight 500
Console(config-router)#
```

Display Information

show ip bgp This command shows entries in the routing table.

SYNTAX

show ip bgp *ip-address* [*netmask* [**longer-prefixes**]]

ip-address – IP address of a route entry.

netmask – Network mask for the route. This mask identifies the network address bits used for the associated routing entries.

longer-prefixes – Specified route and all more specific routes.

COMMAND MODE

Privileged Exec

EXAMPLE

```

Console#show ip bgp
BGP table version is 0, local router ID is 192.168.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i internal,
               r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

      Network          Next Hop          Metric LocPrf Weight Path
*>12.0.0.0             10.1.1.121             0           32768 ?
*>100.1.1.0/24         10.1.1.200             0           32768 ?
*>100.1.2.0/24         10.1.1.200             0           32768 ?
*i192.168.0.0/24      0.0.0.0                0           32768 i

Total number of prefixes 4
Console#

```

Table 197: show ip bgp - display description

Field	Description
BGP table version	Internal version number of routing table, incremented per table change.
local router ID	IP address of router.
Status codes	Status of table entry includes these values: <ul style="list-style-type: none"> ♦ s – Entry is suppressed. ♦ d – Entry is dampened. ♦ h – Entry history ♦ * – Entry is valid ♦ > – Best entry for that network ♦ i – Entry learned via internal BGP (iBGP). ♦ r – Entry is Routing Information Base (RIB) failure ♦ S – Entry is stale. ♦ R – Entry removed.
Origin codes	Origin of table entry includes these values: <ul style="list-style-type: none"> ♦ i – Entry originated from an Interior Gateway Protocol (IGP) and was advertised using a network router configuration command. ♦ e – Entry originated from an Exterior Gateway Protocol (EGP). ♦ ? – Origin of the path undetermined. This normally indicates a route which has been redistributed into BGP from an IGP.
Network	IP address of network entry.
Next Hop	IP address of the next router used to reach destination network.
Metric	Value of inter-autonomous system metric.
LocPrf	Local preference value defined by the set local-preference route-map configuration command.
Weight	Weight of the route determined by autonomous system filters.
Path	Autonomous system paths used to reach the destination network.
Total number of prefixes	Total number of unique route prefixes in the table.

show ip bgp attribute-info This command shows internal attribute hash information.

SYNTAX

show ip bgp attribute-info

COMMAND MODE

Privileged Exec

EXAMPLE

In the following example, Refcnt refers to the number of routes using the indicated next hop.

```
Console#show ip bgp attribute-info
Refcnt  Nexthop
      1 0.0.0.0
      1 10.1.1.64
      3 10.1.1.64
      1 10.1.1.121
      2 10.1.1.200
Console#
```

show ip bgp cidr-only This command shows routes which use classless interdomain routing network masks.

SYNTAX

show ip bgp cidr-only

COMMAND MODE

Privileged Exec

EXAMPLE

This example shows routes that do not match the natural A, B, C or D network masks defined for the earliest IP networks.

```
Console#show ip bgp cidr-only
BGP table version is 0, local router ID is 192.168.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i internal,
               r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop           Metric LocPrf Weight Path
*>3.3.3.0/24        10.10.10.10              0 11 i
*>6.6.6.0/24        0.0.0.0                 32768 i
Console#
```


show ip bgp community This command shows routes that belong to specified BGP communities.

SYNTAX

show ip bgp community [[AA:NN] [internet] [local-as] [no-advertise] [no-export]] [exact-match]]

AA:NN – Standard community-number to match. The 4-byte community number is composed of a 2-byte autonomous system number and a 2-byte network number, separated by one colon. Each 2-byte number can range from 0 from 65535. One or more communities can be entered, separated by a space. Up to 16 community numbers are supported.

internet – Specifies the entire Internet. Routes with this community attribute are advertised to all internal and external peers.

local-as – Specifies the local autonomous system. Routes with this community attribute are advertised only to peers that are part of the local autonomous system or to peers within a sub-autonomous system of a confederation. These routes are not advertised to external peers or to other sub-autonomous systems within a confederation.

no-advertise – Routes with this community attribute are not advertised to any internal or external peer.

no-export – Routes with this community attribute are advertised only to peers in the same autonomous system or to other sub-autonomous systems within a confederation. These routes are not advertised to external peers.

exact-match – Displays only routes that match the specified communities exactly.

COMMAND MODE

Privileged Exec

EXAMPLE

```

Console#show ip bgp community
BGP table version is 0, local router ID is 192.168.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i internal,
               r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop           Metric LocPrf Weight Path
*  100.1.1.0/24      0.0.0.0                      32768 700 800 i
*> 172.0.0.0/8       0.0.0.0                      32768 700 800 i

Total number of prefixes 2
Console#

```

show ip bgp community-info This command shows community messages permitted by BGP.

SYNTAX

show ip bgp community-info

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip bgp community-info
Address      Refcnt  Community
[0x3312558] (3)    100:50
Console#
```

Table 198: show ip bgp community-info - display description

Field	Description
Address	Internal address in memory where the entry is stored.
Refcnt	The number of routes which refer to this community.
Community	4-byte community number composed of a 2-byte autonomous system number and a 2-byte network number, separated by one colon

show ip bgp community-list This command shows the routes matching a community-list.

SYNTAX

show ip bgp community-list {1-99 | 100-500 | *community-list-name*}
[**exact-match**]

1-99 – Standard community list number that identifies one or more groups of communities.

100-500 – Expanded community list number that identifies one or more groups of communities.

community-list-name – Name of standard or expanded access list.
(Maximum length: 32 characters, no spaces or other special characters)

exact-match – Displays only routes that match the specified communities exactly.

COMMAND MODE

Privileged Exec

EXAMPLE

```

Console#show ip bgp community-list rd
BGP table version is 0, local router ID is 192.168.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i internal,
               r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*  100.1.1.0/24      0.0.0.0                          32768 700 800 i
*> 172.0.0.0/8       0.0.0.0                          32768 700 800 i
Console#

```

show ip bgp dampening This command shows dampened routes.

SYNTAX

show ip bgp dampening {dampened-paths | flap-statistics | parameters}

dampened-paths – Routes suppressed due to dampening.

flap-statistics – Statistics for flapping route prefixes.

parameters – Route dampening parameters.

COMMAND MODE

Privileged Exec

EXAMPLE

In the following example, “From” indicates the peer that advertised this path, while “Reuse” is the time after which the path will be made available.

```

Console#show ip bgp dampening dampened-paths
BGP table version is 0, local router ID is 192.168.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i internal,
               r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          From          Reuse      Path
*d 100.1.3.0/24      10.1.1.64      00:27:40 100 ?

Total number of prefixes 1
Console#

```

In this example, “Duration” indicates the time since the first flap occurred.

```

Console#show ip bgp dampening flap-statistics
BGP table version is 0, local router ID is 192.168.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i internal,
               r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          From          Flaps Duration Reuse      Path
*d 100.1.3.0/24      10.1.1.64      3      00:06:05 00:27:00 100 ?

```

```
Total number of prefixes 1
Console#
```

This example shows the dampening parameters configured on this router.

```
Console#show ip bgp dampening parameters
Dampening 15 750 2000 60
  Reachability half-life time      :15 min
  Reuse penalty                    :750
  Suppress penalty                 :2000
  Max suppress time                :60 min
Console#
```

Table 199: show ip bgp dampening parameters- display description

Field	Description
Reachability half-life time	The time after which a penalty is reduced. The penalty value is reduced to half of the previous value after the half-life time expires.
Reuse penalty	The point to which the penalty for a flapping route must fall before a route is unsuppressed.
Suppress penalty	The point at which to start suppressing a route.
Max suppress time	The maximum time a route can be suppressed.

show ip bgp filter-list This command shows routes matching the specified filter list.

SYNTAX

show ip bgp filter-list *access-list-name*

access-list-name – Name of a list of autonomous system paths as defined by the [ip as-path access-list](#) command. (Maximum length: 16 characters, no spaces or other special characters)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip bgp filter-list rd
BGP table version is 0, local router ID is 192.168.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i internal,
               r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop           Metric LocPrf Weight Path
*> 100.1.1.0/24      10.1.1.64                0             0 100 ?
Total number of prefixes 1
Console#
```

show ip bgp neighbors This command shows connection information for neighbor sessions.

SYNTAX

show ip bgp neighbors [*ip-address*] [**advertised-routes** | **received prefix-filter** | **received-routes** | **routes**]

ip-address – IP address of the neighbor.

advertised-routes – Shows the routes advertised to a neighbor.

received prefix-filter – Shows the prefix-list (outbound route filter) sent from a neighbor.

received-routes – Shows all routes, both accepted and rejected, which have been received from a neighbor. To display all received routes from a neighbor, first enable soft reconfiguration with the [neighbor soft-reconfiguration inbound](#) command.

routes – Displays all accepted routes learned from a neighbor.

COMMAND MODE

Privileged Exec

```

Console#show ip bgp neighbors 192.168.0.3
BGP neighbor is 192.168.0.3, remote AS 200, local AS 100, external link
Member of peer-group for session parameters
BGP version 4, remote router ID 192.168.0.3
BGP state = Established, up for 00:00:58
Last read 16:40:37, hold time is 180, keepalive interval is 60 seconds
Neighbor capabilities:
  4 Byte AS: advertised and received
  Route refresh: advertised and received(old & new)
  Address family IPv4 Unicast: advertised and received
Message statistics:
  Inq depth is 0
  Outq depth is 0

              Sent          Rcvd
Opens:                1            0
Notifications:        0            0
Updates:              1            1
Keepalives:           2            1
Route Refresh:         0            0
Capability:            0            0
Total:                 4            2
Minimum time between advertisement runs is 30 seconds

For address family: IPv4 Unicast
Community attribute sent to this neighbor(both)
Inbound path policy configured
1 accepted prefixes

Connections established 1; dropped 0
Last reset never
Local host: 192.168.0.2, Local port: 179
Foreign host: 192.168.0.3, Foreign port: 3987
Next hop:
Read thread: on  Write thread: off

```

Console#

Table 200: show ip bgp - display description

Field	Description
BGP neighbor	IP address of neighbor.
remote AS	Autonomous system number of the neighbor.
local AS	Local autonomous system number.
external link	"external link" is displayed for external BGP neighbors. "internal link" is displayed for iBGP neighbors.
BGP version	BGP version used to communicate with remote router.
remote router ID	IP address of the neighbor.
BGP state	Stage of session negotiation.
Last read	Time since a message was last received from this neighbor.
hold time	Time to maintain the session with this neighbor without receiving a message.
keepalive interval	Interval at which keepalive messages are transmitted to this neighbor.
Neighbor capabilities	BGP capabilities advertised and received from this neighbor.
Message statistics	Statistics organized by message type.
Minimum time between advertisement runs	Time between transmission of advertisements.
For address family	Address family to which the following information refers.
Local host/port	IP address and TCP port of the local BGP speaker.
Foreign host/port	IP address and TCP port of the neighbor BGP speaker.
Nexthop	IP address of next system via which packets are forwarded to the destination network.
Read thread	The read status for the socket connection with this neighbor.
Write thread	The write status for the socket connection with this neighbor.

show ip bgp paths This command shows all paths in the database.

SYNTAX

show ip bgp paths

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip bgp paths
Address      RefCnt  ASpath
0x331dad0:0  1
0x331d850:93 1  600
```

```
0x331d8d8:249      2   200 300
Console#
```

Table 201: show ip bgp paths - display description

Field	Description
Address	Internal address in memory where the path is stored.
Refcnt	The number of routes using this path.
ASpath	The autonomous system path for this route.

show ip bgp prefix-list This command shows routes matching the specified prefix-list.

SYNTAX

show ip bgp prefix-list *list-name*

list-name – Name of a prefix-list. The prefix list can be used to filter the networks to import or export as defined by the [match ip address prefix-list](#) command. (Range: 1-80 characters)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip bgp prefix-list rd
BGP table version is 0, local router ID is 192.168.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i internal,
               r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop           Metric LocPrf Weight Path
*  100.1.1.0/24      10.1.1.66              0         0 200 300 ?
*>                  10.1.1.100             0         32768 ?
Console#
```

show ip bgp regexp This command shows routes matching the AS path regular expression.

SYNTAX

show ip bgp regexp *regular-expression*

regular-expression – Regular expression indicating the path attributes to match. Syntax complies with the IEEE POSIX Basic Regular Expressions (BRE) standard.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip bgp regexp 100
BGP table version is 0, local router ID is 192.168.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i internal,
               r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*  100.1.1.0/24      10.1.1.64              0           0 500 100 600 ?
Console#
```

show ip bgp route-map This command shows routes matching the specified route map.

SYNTAX

show ip bgp route-map *map-name*

map-name – Name of the route map as defined by the [route-map](#) command. The route map can be used to filter the networks to advertise. (Range: 1-80 characters)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip bgp route-map rd
BGP table version is 0, local router ID is 192.168.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i internal,
               r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*  100.1.1.0/24      10.1.1.64              0           0 500 100 600 ?
*> 10.1.1.68         10.1.1.68              0           0 300 ?
Console#
```

show ip bgp scan This command shows BGP scan status.

SYNTAX

show ip bgp scan

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip bgp scan
BGP scan is running
BGP scan interval is 60
Current BGP nexthop cache:
 10.10.10.64 valid [IGP metric 0]
BGP connected route:
 10.10.10.0/24
 10.10.11.0/24
Console#
```

show ip bgp summary This command shows summary information for all connections.

SYNTAX

show ip bgp summary

COMMAND MODE

Privileged Exec

EXAMPLE

In the following example, “Up/Down” refers to the length of time the session has been in the Established state, or the current status if not in Established state.

```
Console#show ip bgp summary
BGP router identifier 192.168.0.2, local AS number 100
RIB entries 0
Peers 1
Peer groups 0
Neighbor      V    AS MsgRcvd MsgSent  TblVer  InQ  OutQ Up/Down  State/PfxRcd
192.168.0.3    4    200    166    168        0     0     0 02:45:00      1

Total number of neighbors 1

Console#
```

show ip community-list This command shows routes permitted by a community list.

SYNTAX

show ip community-list [1-99 | 100-500 | *community-list-name*]

1-99 – Standard community list number that identifies one or more groups of communities.

100-500 – Expanded community list number that identifies one or more groups of communities.

community-list-name – Name of standard or expanded access list.
(Maximum length: 32 characters, no spaces or other special characters)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip community-list rd
Named Community standard list rd
  permit 100:10
Console#
```

show ip extcommunity-list This command shows routes permitted by an extended community list.

SYNTAX

show ip extcommunity-list [1-99 | 100-500 | *community-list-name*]

1-99 – Standard community list number that identifies one or more groups of communities.

100-500 – Expanded community list number that identifies one or more groups of communities.

community-list-name – Name of standard or expanded access list.
(Maximum length: 32 characters, no spaces or other special characters)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip extcommunity-list rd
Named extended community standard list rd
  permit RT:192.168.0.0:10
Console#
```

show ip prefix-list This command shows the specified prefix list.

SYNTAX

show ip prefix-list [*prefix-list-name* [*ip-address netmask* [**first-match** | **longer**] | **seq** *sequence-number*]]

prefix-list-name – Name of prefix list. (Maximum length: 128 characters, no spaces or other special characters)

ip-address – An IPv4 address expressed in dotted decimal notation.

netmask – Network mask for the route. This mask identifies the network address bits used for the associated routing entries.

first-match – First matched prefix.

longer – All entries more specific than the specified network/mask.

sequence-number – The sequence number of an entry.
(Range: 1-429496725)

COMMAND MODE
Privileged Exec

EXAMPLE

```
Console#show ip prefix-list rd
ip prefix-list rd: 1 entries
  seq 5 deny 10.0.0.0/8 ge 14 le 22
Console#
```

show ip prefix-list detail This command shows detailed information for the specified prefix list.

SYNTAX

show ip prefix-list detail [*prefix-list-name*]

prefix-list-name – Name of prefix list. (Maximum length: 128 characters, no spaces or other special characters)

COMMAND MODE
Privileged Exec

EXAMPLE

```
Console#show ip prefix-list detail rd
ip prefix-list rd:
  count: 1, range entries: 0, sequences: 5 - 5
  seq 5 deny 10.0.0.0/8 ge 14 le 22 (hit count: 0, refcount: 0)
Console#
```

show ip prefix-list summary This command shows summary information for the specified prefix list.

SYNTAX

show ip prefix-list summary [*prefix-list-name*]

prefix-list-name – Name of prefix list. (Maximum length: 128 characters, no spaces or other special characters)

COMMAND MODE
Privileged Exec

EXAMPLE

```
Console#show ip prefix-list summary rd
ip prefix-list rd:
```

```
count: 1, range entries: 0, sequences: 5 - 5  
Console#
```

POLICY-BASED ROUTING FOR BGP

This section describes commands used to configure policy-based routing (PBR) maps for Border Gateway Protocol (BGP).

Policy-based routing is performed before regular routing. PBR inspects traffic on the interface where the policy is applied and then, based on the policy, makes some decision. First, the traffic is “matched” according to the policy. Second, for each match, there is something “set.” What is set could be that the traffic matches must exit out a different interface, or the traffic could be given a higher priority, or it could choose to just drop that traffic.

Matching of the traffic is usually done with an ACL (access-control list) that is referenced by a route-map. In the route-map, if there is a “match” for the traffic defined in that ACL, then a “set” defines what the administrator wants to happen to that traffic (prioritize it, route it differently, drop it, or other actions). Policies can be based on IP address, port numbers, protocols, or size of packets.

If matching criteria is found and the specified action is to permit the packet, then it will be forwarded to the next hop based on policy-based routing. If the action is to deny the packet, normal unicast routing is used to determine the packet’s next hop, instead of using policy-based routing. If no matching criteria are found in the route map, normal unicast routing is used to determine the packet’s next hop. Although route redistribution is protocol-independent, some of the route-map match and set commands defined in this section are specific to BGP.

Like matches in the same route map subblock are filtered with “or” semantics. If any one match clause is matched in the entire route map subblock, this match is treated as a successful match. Dissimilar match clauses are filtered with “and” semantics. If the first set of conditions is not met, the second match clause is filtered. This process continues until a match occurs or there are no more match clauses.

A route map can have several sequences. A route that does not match at least one match command defined in a route-map will be ignored; that is, the route will not be advertised for outbound route maps nor accepted for inbound route maps.

Table 202: Policy-based Routing Configuration Commands

Command	Function	Mode
<code>route-map</code>	Enters route-map configuration mode, allowing route maps to be created or modified	GC
<code>call</code>	Jumps to another route map after match and set commands are executed	RM
<code>continue</code>	Goes to a route-map entry with a higher sequence number after a successful match occurs	RM
<code>description</code>	Creates a description of an entry in the route map	RM

Table 202: Policy-based Routing Configuration Commands (Continued)

Command	Function	Mode
match as-path	Sets an AS path access list to match	RM
match community	Sets a BGP community access list to match	RM
match extcommunity	Sets a BGP extended community access list to match	RM
match ip address	Specifies destination addresses to match in a standard access list, extended access list, or prefix list	RM
match ip next-hop	Specifies next hop addresses to match in a standard access list, extended access list, or prefix list	RM
match ip route-source	Specifies the source of routing messages to match in a standard access list, extended access list, or prefix list	RM
match metric	Sets the metric value to match in routing messages	RM
match origin	Sets the originating protocol to match in routing messages	RM
match pathlimit	Sets the maximum AS path length for propagation of more specific prefixes to match in routing messages	RM
match peer	Sets the peer address to match in routing messages	RM
on-match	Sets the next entry to go to when this entry matches	RM
set aggregator as	Assigns an AS number and IP address to the aggregator attribute of a route	RM
set as-path	Modifies the AS path by prepending or excluding an AS number	RM
set atomic-aggregate	Indicates the loss of some information in the route aggregation process	RM
set comm-list delete	Removes communities from the community attribute of inbound or outbound routing messages	RM
set community	Sets the community attributes of routing messages	RM
set extcommunity	Sets the extended community attributes of routing messages	RM
set ip next-hop	Sets the next-hop for a routing message	RM
set local-preference	Sets the priority within the local AS for a routing message	RM
set metric	Sets the metric value of a route to external neighbors	RM
set origin	Sets the origin code for the routing protocol which generated this message	RM
set originator-id	Sets the IP address of the routing message's originator	RM
set pathlimit ttl	Sets the maximum AS path length for propagation of more specific prefixes in routing messages	RM
set weight	Sets the weight for routing messages	RM
show route-map	Shows the configuration setting for a route map	PE

route-map This command enters route-map configuration mode, allowing route maps to be created or modified. Use the **no** form to remove a route map.

SYNTAX

[no] route-map *map-name* {**deny** | **permit**} *sequence-number*

map-name – Name for the route map. (Range: 1-128 case-sensitive alphanumeric characters)

deny – Route-map denies set operations.

permit – Route-map permits set operations.

sequence-number – Sequence to insert to or delete from existing route-map entry. (Range: 1-65535)

COMMAND MODE

Global Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

- ◆ This command enters the route map configuration mode. In this mode, a new route map can be created, or an existing route map modified.
- ◆ The match commands specify the conditions under which policy routing occurs, and the set commands specify the routing actions to perform if the criteria enforced by the match commands are met.
- ◆ If the match criteria are met for a route map, and the permit keyword specified, the packet is policy routed based on defined set commands.
- ◆ If the match criteria are not met, and the permit keyword specified, the next route map with the same map-name is tested. If a route passes none of the match criteria for the set of route maps sharing the same name, it is not policy routed by that set.
- ◆ If the match criteria are met for the route map and the deny keyword specified, the packet is not policy routed, and no further route maps sharing the same map-name are examined. If the packet is not policy routed, the normal forwarding process is used.
- ◆ Processing for exceptions include the following results:
 - For a deny route-map, if it does not have a match clause, any routing message is matched, and therefore all routes are denied.
 - For a deny route-map which includes a match clause for an access-list, if the access-list does not exist, no routing message will be matched, and therefore all routes are skipped.

- For a permit route-map, if it does not have a match clause, any routing message is matched, and therefore all routes are permitted.
- For a permit route-map which includes a match clause for an access-list, if the access-list does not exist, no routing messages are matched, and therefore all routes are skipped.

EXAMPLE

```
Console(config)#route-map r1 permit 1
Console(config-route-map)#match as-path 60
Console(config-route-map)#set weight 30
Console(config-route-map)#
```

call This command jumps to another route map after match and set commands are executed. Use the **no** form to remove an entry from a route map.

SYNTAX

call *map-name*

no call

map-name – Name for the route map. (Range: 1-128 case-sensitive alphanumeric characters)

COMMAND MODE

Route Map

COMMAND USAGE

Only one call clause is permitted per route map. The call clause executed only after all match and set commands are executed.

EXAMPLE

```
Console(config)#route-map r1 permit 1
Console(config-route-map)#match as-path 60
Console(config-route-map)#set weight 30
Console(config-route-map)#call FD
Console(config-route-map)#
```

continue This command goes to a route-map entry with a higher sequence number after a successful match occurs. Use the **no** form to remove this entry from a route map.

SYNTAX

continue [*sequence-number*]

no continue

sequence-number – Sequence number at which to continue processing.
(Range: 1-65535)

COMMAND MODE

Route Map

COMMAND USAGE

If no match statements precede the call entry, the call is automatically executed. If no sequence number is specified by the call entry, the next entry is executed.

EXAMPLE

```
Console(config)#route-map RD permit 1
Console(config-route-map)#match as-path 60
Console(config-route-map)#set weight 30
Console(config-route-map)#continue 3
Console(config-route-map)#
```

description This command creates a description of an entry in the route map. Use the **no** form to remove the description.

SYNTAX

description *text*

no description

text – Comment describing this route-map rule. (Maximum length: 128 characters, no spaces or other special characters)

COMMAND MODE

Route Map

EXAMPLE

```
Console(config)#route-map RD permit 1
Console(config-route-map)#description AS-Path rule
Console(config-route-map)#match as-path 60
Console(config-route-map)#set weight 30
Console(config-route-map)#
```


match as-path This command sets a BGP autonomous system path access list to match. Use the **no** form to remove this entry from a route map.

SYNTAX

[no] match as-path *access-list-name*

access-list-name – Name of the access list. (Maximum length: 16 characters, no spaces or other special characters)

COMMAND MODE

Route Map

COMMAND USAGE

The weights assigned by the **match as-path** and **set weight** route-map commands command override the weight assigned using the BGP **neighbor weight** command.

EXAMPLE

```
Console(config)#route-map RD permit 1
Console(config-route-map)#match as-path 60
Console(config-route-map)#set weight 30
Console(config-route-map)#
```

RELATED COMMANDS

[ip as-path access-list \(922\)](#)

match community This command sets a BGP community access list to match. Use the **no** form to remove this entry from a route map.

SYNTAX

match community {1-99 | 100-500 | *community-list-name*} [**exact-match**]

no match community

1-99 – Standard community list number that identifies one or more groups of communities.

100-500 – Expanded community list number that identifies one or more groups of communities.

community-list-name – Name of standard or expanded community list. (Maximum length: 32 characters, no spaces or other special characters)

exact-match – Must exactly match the specified community list. All and only those communities specified must be present.

COMMAND MODE

Route Map

COMMAND USAGE

This command matches the community attributes of the BGP routing message following the rules specified with the [ip community-list](#) command.

EXAMPLE

```
Console(config)#route-map RD permit 2
Console(config-route-map)#match community 60
Console(config-route-map)#set weight 30
Console(config-route-map)#
```

match extcommunity This command sets a BGP extended community access list to match. Use the **no** form to remove this entry from a route map.

SYNTAX

match extcommunity {1-99 | 100-500} [**exact-match**]

no match extcommunity

1-99 – Standard community list number that identifies one or more groups of communities.

100-500 – Expanded community list number that identifies one or more groups of communities.

COMMAND MODE

Route Map

COMMAND USAGE

This command matches the extended community attributes of the BGP routing message following the rules specified with the [ip extcommunity-list](#) command.

EXAMPLE

```
Console(config)#route-map RD permit 3
Console(config-route-map)#match extcommunity 160
Console(config-route-map)#set weight 30
Console(config-route-map)#
```

match ip address This command specifies the destination addresses to be matched in a standard access list, an extended access list, or a prefix list. Use the **no** form to remove this entry from a route map.

SYNTAX

match ip address {*access-list-name* | **prefix-list** *prefix-list-name*}

no match ip address

access-list-name – Name of standard or extended access list.
(Maximum length: 32 characters, no spaces or other special characters)

prefix-list-name – Name of a specific prefix list.

COMMAND MODE

Route Map

EXAMPLE

```
Console(config)#route-map RD permit 4
Console(config-route-map)#match ip address rd-addresses
Console(config-route-map)#set weight 30
Console(config-route-map)#
```

RELATED COMMANDS

[ip prefix-list \(927\)](#)

[Access Control Lists \(347\)](#)

match ip next-hop This command specifies the next-hop addresses to be matched in a standard access list, an extended access list, or a prefix list. Use the **no** form to remove this entry from a route map.

SYNTAX

match ip next-hop {*access-list-name* | **prefix-list** *prefix-list-name*}

no match ip next-hop

access-list-name – Name of standard or extended access list.
(Maximum length: 32 characters, no spaces or other special characters)

prefix-list-name – Name of a specific prefix list.

COMMAND MODE

Route Map

COMMAND USAGE

When inbound update messages are received from a neighbor, next-hop information contained in Network Layer Reachability Information (NLRI) entries is checked against the specified access-list or prefix-list before any routes are learned.

EXAMPLE

```
Console(config)#route-map RD permit 5
Console(config-route-map)#match ip next-hop rd-next-hops
Console(config-route-map)#set weight 30
Console(config-route-map)#
```

match ip route-source This command specifies the source of routing messages advertised by routers and access servers to be matched in a standard access list, an extended access list, or a prefix list. Use the **no** form to remove this entry from a route map.

SYNTAX

match ip route-source {*access-list-name* | **prefix-list** *prefix-list-name*}

no match ip route-source [*access-list-name* | **prefix-list**]

access-list-name – Name of standard or extended access list.
(Maximum length: 32 characters, no spaces or other special characters)

prefix-list-name – Name of a specific prefix list.

COMMAND MODE

Route Map

COMMAND USAGE

Note that there may be situations in which the next hop and source router address of the route are not the same.

EXAMPLE

```
Console(config)#route-map RD permit 6
Console(config-route-map)#match ip route-source rd-sources
Console(config-route-map)#set weight 30
Console(config-route-map)#
```

match metric This command sets the metric value to match in routing messages. Use the **no** form to remove this entry from a route map.

SYNTAX

match metric *metric-value*

no match metric

metric-value – The metric value in the routing messages.
(Range: 0-4294967295)

COMMAND MODE

Route Map

EXAMPLE

```
Console(config)#route-map RD permit 7
Console(config-route-map)#match metric 60
Console(config-route-map)#set weight 30
Console(config-route-map)#
```

match origin This command sets the originating protocol to match in routing messages. Use the **no** form to remove this entry from a route map.

SYNTAX

match origin {egp | igp | incomplete}

no match origin

egp – Routes learned from exterior gateway protocols.

igp – Routes learned from internal gateway protocols.

incomplete – Routes of uncertain origin.

COMMAND MODE

Route Map

EXAMPLE

```
Console(config)#route-map RD permit 8
Console(config-route-map)#match origin igp
Console(config-route-map)#set weight 30
Console(config-route-map)#
```

match pathlimit This command sets the maximum AS path length allowed for propagation of more specific prefixes to match in routing messages. Use the **no** form to remove this entry from a route map.

SYNTAX

match pathlimit as *as-limit*

no match pathlimit as

as-limit – Maximum AS path length. (Range: 1-65535)

COMMAND MODE

Route Map

COMMAND USAGE

- ◆ To perform inter-domain traffic engineering, a multi-homed site can advertise its prefix to all of its neighbors via an aggregate address, and also advertise more specific prefixes to a subset of its neighbors. The longest match lookup

algorithm then causes traffic for the more specific prefixes to be forwarded to the subset of neighbors with the more specific prefix.

These longer prefixes may be advertised in addition to an aggregate, even when the aggregate advertisement is sufficient for basic reachability. This type of inter-domain traffic engineering is a widely used phenomenon that is contributing to growth in the size of the global routing table.

Traffic engineering via longer prefixes is only effective when the longer prefixes have a different next hop from the less specific prefix. Thus, past the point where the next hops become identical, the longer prefixes provide no value whatsoever. This command can be used to limit the radius of propagation of more specific prefixes by adding a count of the ASes that may be traversed by the more specific prefix.

- ◆ Private AS numbers [RFC1930] and confederation AS members [RFC3065] found in the AS_PATH are not counted. AS numbers found within an AS_SET are not counted and an entire AS_SET is counted as a single AS. Each instance of an AS number that appears multiple times in an AS_PATH is counted.

If the AS_PATHLIMIT attribute is attached to a prefix by a private AS, then when the prefix is advertised outside of the parent AS, the AS number contained in the AS_PATHLIMIT attribute should be replaced by the AS number of the parent AS.

Similarly, if the AS_PATHLIMIT attribute is attached to a prefix by a member of a confederation, then when the prefix is advertised outside of the confederation boundary, then the AS number of the confederation member inside of the AS_PATHLIMIT attribute should be replaced by the confederation's AS number.

EXAMPLE

```
Console(config)#route-map RD permit 8
Console(config-route-map)#match pathlimit as 5
Console(config-route-map)#on match goto 20
Console(config-route-map)#
```

match peer This command sets the peer address to match in routing messages. Use the **no** form to remove this entry from a route map.

SYNTAX

match peer {*peer-address* | **local**}

no match peer [*peer-address* | **local**]

peer-address – IP address of neighboring router sending routing messages.

local – Static or redistributed routes.

COMMAND MODE

Route Map

EXAMPLE

```
Console(config)#route-map RD permit 9
Console(config-route-map)#match peer 192.168.0.99
Console(config-route-map)#set weight 30
Console(config-route-map)#
```

on-match This command sets the next entry to go to when this entry matches. Use the **no** form to remove this entry from a route map.

SYNTAX

on-match peer {**goto** *sequence-number* | **next**}

no on-match peer {**goto** | **next**}

goto – On match, go to specified entry.

sequence-number – Route-map entry. (Range: 1-65535)

next – Go to next entry.

COMMAND MODE

Route Map

COMMAND USAGE

Use this command when no set action is for a match clause.

EXAMPLE

```
Console(config)#route-map RD permit 8
Console(config-route-map)#match pathlimit as 5
Console(config-route-map)#on match goto 20
Console(config-route-map)#
```

set aggregator as This command assigns an AS number and IP address to the aggregator attribute of a route. Use the **no** form to remove this entry from a route map.

SYNTAX

set aggregator as *as-number ip-address*

no set aggregator as [*as-number ip-address*]

as-number – Autonomous system number. (Range: 1-4294967295)

ip-address – IP address of aggregator.

COMMAND MODE

Route Map

COMMAND USAGE

Aggregate routes advertised to a neighbor contain an aggregator attribute. This attribute contains an AS number and IP address. The AS number is the creator's AS number (or confed ID in a confederation) and an IP address which is the creator's router-id. The **set aggregator as** command can be used to overwrite the aggregator attribute in routes created locally with the [aggregate-address](#) command, or in routes learned from a neighbor which already carry an aggregator attribute, or to add a new aggregator attribute to a route which has no aggregator attribute.

EXAMPLE

```
Console(config)#route-map RD permit 8
Console(config-route-map)#match pathlimit as 5
Console(config-route-map)#set aggregator 1 192.168.0.0
Console(config-route-map)#
```

set as-path This command modifies the AS path by prepending or excluding an AS number. Use the **no** form to remove this entry from a route map.

SYNTAX

set as-path {exclude | prepend} as-number...

no set as-path {exclude | prepend}

exclude – Removes one or more autonomous system numbers from the AS path of the route that is matched.

prepend – Appends one or more autonomous system numbers to the AS path of the route that is matched.

as-number – Autonomous system number. (Range: 1-4294967295)

COMMAND MODE

Route Map

COMMAND USAGE

Note that best path selection may be influenced with this command by varying the length of the autonomous system path.

EXAMPLE

```
Console(config)#route-map RD permit 8
Console(config-route-map)#match peer 192.168.0.99
Console(config-route-map)#set as-path prepend 2
Console(config-route-map)#
```


set atomic-aggregate This command indicates the loss of some information in the route aggregation process. Use the **no** form to remove this entry from a route map.

SYNTAX

[no] set atomic-aggregate

COMMAND MODE

Route Map

COMMAND USAGE

The purpose of the atomic-aggregate attribute is to alert BGP speakers along the path that some information have been lost due to the route aggregation process and that the aggregate path might not be the best path to the destination. This attribute should be set when the BGP speaker advertises ONLY the less-specific prefix and suppresses more specific ones.

EXAMPLE

```
Console(config)#route-map RD permit 9
Console(config-route-map)#match peer 192.168.0.99
Console(config-route-map)#set atomic-aggregate
Console(config-route-map)#
```

set comm-list delete This command removes communities from the community attribute of inbound or outbound routing messages. Use the **no** form to remove this entry from a route map.

SYNTAX

[no] set comm-list {1-99 | 100-500 | *community-list-name*} [delete]

1-99 – Standard community list number that identifies one or more groups of communities.

100-500 – Expanded community list number that identifies one or more groups of communities.

community-list-name – Name of standard or expanded community list.
(Maximum length: 32 characters, no spaces or other special characters)

COMMAND MODE

Route Map

COMMAND USAGE

When using the [ip community-list](#) command to configure a community access list, each entry of a standard community list should list only one community.

Otherwise, the **set comm-list delete** command will not succeed. For example, in order to be able to delete communities 100 and 200, you must create two separate entries with the [ip community-list](#) command.

EXAMPLE

```
Console(config)#route-map RD permit 10
Console(config-route-map)#match peer 192.168.0.77
Console(config-route-map)#set comm-list 10:01 delete
Console(config-route-map)#exit
Console(config)#route-map RD permit 11
Console(config-route-map)#match peer 192.168.0.99
Console(config-route-map)#set comm-list 20:01 delete
Console(config-route-map)#
```

set community This command sets the community attributes of routing messages. Use the **no** form to remove this entry from a route map.

SYNTAX

set community

```
[AA:NN...]
[additive [[AA:NN...] [internet] [local-as] [no-advertise] [no-export]]
[internet [[AA:NN...] [local-as] [no-advertise] [no-export]]
[local-as [[AA:NN...] [no-advertise] [no-export]]
[no-advertise [AA:NN...] [no-export]]
[no-export [AA:NN...]]
[none]
```

no set community

AA:NN – Standard community-number. The 4-byte community number is composed of a 2-byte autonomous system number and a 2-byte network number, separated by one colon. Each 2-byte number can range from 0 from 65535. One or more communities can be entered, separated by a space. Up to 16 community numbers are supported.

additive – Adds community attributes to already existing community attributes.

internet – Specifies the entire Internet. Routes with this community attribute are advertised to all internal and external peers.

local-as – Specifies the local autonomous system. Routes with this community attribute are advertised only to peers that are part of the local autonomous system or to peers within a sub-autonomous system of a confederation. These routes are not advertised to external peers or to other sub-autonomous systems within a confederation.

no-advertise – Routes with this community attribute are not advertised to any internal or external peer.

no-export – Routes with this community attribute are advertised only to peers in the same autonomous system or to other sub-autonomous systems within a confederation. These routes are not advertised to external peers.

none – Delete the community attributes from the prefix of this route.

COMMAND MODE

Route Map

EXAMPLE

```
Console(config)#route-map RD permit 11
Console(config-route-map)#match peer 192.168.0.99
Console(config-route-map)#set community 10:01
Console(config-route-map)#exit
Console(config)#route-map RD permit 12
Console(config-route-map)#match peer 192.168.0.99
Console(config-route-map)#set community 20:01
Console(config-route-map)#
```

RELATED COMMANDS

[set comm-list delete \(1001\)](#)

set extcommunity This command sets the extended community attributes of routing messages. Use the **no** form to remove this entry from a route map.

SYNTAX

set extcommunity {**rt** *extended-community-value* |
soo *extended-community-value*}

no set extcommunity [**rt** | **soo**]

rt – The route target extended community attribute.

soo – The site of origin extended community attribute.

extended-community-value – The route target or site of origin in one of the following formats:

AAAA:NN or *AA:NNNN* – Community-number to deny or permit. The community number can either be formatted as a 4-byte autonomous system number and a 2-byte network number, or as a 2-byte autonomous system number and a 4-byte network number, separated by one colon. Each 2-byte number can range from 0 to 65535, and 4-byte numbers from 0 to 4294967295.

IP:NN – Community to deny or permit. The community number is composed of a 4-byte IP address (representing the autonomous system number) and a 2-byte network number, separated by one colon. The 2-byte network number can range from 0 to 65535.

One or more community numbers can be entered, separated by a space. Up to 3 community numbers are supported.

COMMAND MODE

Route Map

COMMAND USAGE

- ◆ Using the **rt** keyword to specify new route targets replaces existing route targets.
- ◆ The route target (RT) attribute is used to identify sites that may receive routes tagged with a specific route target. Using this attribute allows that route to be placed in per-site forwarding tables used for routing traffic received from the corresponding sites.
- ◆ The site of origin (SOO) attribute is used to identify the site from which the provider edge (PE) router learned the route. All routes learned from a particular site are assigned the same site of origin attribute, no matter if a site is connected to a single PE router or multiple PE routers. Filtering based on this extended community attribute can prevent routing loops from occurring when a site is multi-homed.

EXAMPLE

```
Console(config)#route-map RD permit 13
Console(config-route-map)#match peer 192.168.0.99
Console(config-route-map)#set extcommunity 100:0 192.168.1.1:1
Console(config-route-map)#
```

set ip next-hop This command sets the next-hop for a routing message. Use the **no** form to remove this entry from a route map.

SYNTAX

set ip next-hop {*ip-address* | **peer-address**}

no set ip next-hop [*ip-address*]

ip-address – An IPv4 address of the next hop, expressed in dotted decimal notation.

peer-address – Sets the next hop as the BGP peering address.

COMMAND MODE

Route Map

COMMAND USAGE

- ◆ The IP address specified as the next hop need not be an adjacent router.
- ◆ When this command is used with the **peer-address** keyword in an inbound route map received from a BGP peer, the next hop of the received matching routes are set to be the neighbor peer address, overriding any other next hops.
- ◆ When this command is used with the **peer-address** keyword in an outbound route map for a BGP peer, the next hop of the advertised matching routes will be set to be the peering address of the local router, thus disabling next hop calculation. This command therefore has finer granularity than the [neighbor](#)

`next-hop-self` command, because it can set the next hop for some routes, but not others. While the `neighbor next-hop-self` command sets the next hop for all routes sent to the specified neighbor(s).

EXAMPLE

```
Console(config)#route-map RD permit 14
Console(config-route-map)#match peer 192.168.0.99
Console(config-route-map)#set ip next-hop 192.168.0.254
Console(config-route-map)#
```

set local-preference This command sets the priority within the local AS for a routing message. Use the **no** form to remove this entry from a route map.

SYNTAX

set local-preference *preference*

no set local-preference

preference – Degree of preference iBGP peers give local routes during BGP best path selection. The higher the value, the more the route is to be preferred. (Range: 1-4294967295)

COMMAND MODE

Route Map

COMMAND USAGE

- ◆ The preference is sent only to routers in the local autonomous system. To specify the metric for inter-autonomous systems, use the `set metric` command.
- ◆ A route with a higher local priority level when compared with other routes to the same destination will be preferred over other routes.

EXAMPLE

```
Console(config)#route-map RD permit 15
Console(config-route-map)#match peer 192.168.0.99
Console(config-route-map)#set local-preference 2
Console(config-route-map)#
```

set metric This command sets the metric value of a route to external neighbors. Use the **no** form to restore the default value.

SYNTAX

set metric [+ | -]*metric-value*

no set metric

metric-value – Metric value assigned to all external routes for the specified protocol. (Range: 0-4294967295)

DEFAULT SETTING

The dynamically learned metric value.

COMMAND MODE

Route Map

COMMAND USAGE

- ◆ Lower metric values indicate a higher priority.
- ◆ This command can modify the current metric for a route using the "+" or "-" keywords.
- ◆ The metric applies to external routers in the inter-autonomous system. To specify the metric for the local AS, use the [set local-preference](#) command.
- ◆ This path metric is normally only compared with neighbors in the local AS. To extend the comparison to paths advertised from neighbors in different autonomous systems, use the [bgp always-compare-med](#) command.

EXAMPLE

```
Console(config)#route-map RD permit 16
Console(config-route-map)#match peer 192.168.0.99
Console(config-route-map)#set metric +1
Console(config-route-map)#
```

set origin This command sets the BGP origin code for the routing protocol which generated this message. Use the **no** form to remove this entry from a route map.

SYNTAX

set origin {**egp** | **igp** | **incomplete**}

no set origin

egp – Exterior gateway protocols.

igp – Interior gateway protocols.

incomplete – Route origin unknown.

DEFAULT SETTING

As indicated in main IP routing table

COMMAND MODE

Route Map

COMMAND USAGE

EGP is an inter-domain routing protocol which has been superceded by BGP. IGP indicates any intra-domain routing protocol such as RIP or OSPF.

EXAMPLE

```
Console(config)#route-map RD permit 16
Console(config-route-map)#match peer 192.168.0.99
Console(config-route-map)#set origin egp
Console(config-route-map)#
```

set originator-id This command sets the IP address of the routing message's originator. Use the **no** form to remove this entry from a route map.

SYNTAX

set originator-id *ip-address*

no set originator-id

ip-address – An IPv4 address of the route source, expressed in dotted decimal notation.

COMMAND MODE

Route Map

COMMAND USAGE

This attribute is commonly used for loop prevention by rejecting updates that contain the receiving router's own router-ID in the originator-ID attribute.

EXAMPLE

```
Console(config)#route-map RD permit 17
Console(config-route-map)#match peer 192.168.0.99
Console(config-route-map)#set originator-id 192.168.0.254
Console(config-route-map)#
```

set pathlimit ttl This command sets the maximum AS path length for propagation of more specific prefixes in routing messages. Use the **no** form to remove this entry from a route map.

SYNTAX

set pathlimit ttl *ttl-value*

no set pathlimit ttl

ttl-value – Maximum number of router hops allowed in an AS path.
(Range: 1-255)

COMMAND MODE

Route Map

COMMAND USAGE

Due to the dynamic changes in connections for network paths, it is not advisable to restrict the number of router hops for any path. However, if the connections to the destination network are relatively stable, the hop count can be restricted to force traffic to follow an alternate path. This method may be used to avoid less heavily congested paths or to route traffic through a preferred provider.

EXAMPLE

```
Console(config)#route-map RD permit 18
Console(config-route-map)#match peer 192.168.0.99
Console(config-route-map)#set pathlimit ttl 255
Console(config-route-map)#
```

set weight This command sets the weight for routing messages. Use the **no** form to remove this entry from a route map.

SYNTAX

set weight *weight*

no set weight

weight – The weight assigned to this route. (Range: 0-4294967295)

COMMAND MODE

Route Map

COMMAND USAGE

- ◆ Weights are used to determine the best path available to the local switch. The route with the highest weight gets preference over other routes to the same network.
- ◆ Weights assigned using this command override those assigned by the [neighbor weight](#) command.

EXAMPLE

```
Console(config)#route-map RD permit 19
Console(config-route-map)#match peer 192.168.0.99
Console(config-route-map)#set weight 255
Console(config-route-map)#
```

show route-map This command shows the configuration setting for a route map.

SYNTAX

show route-map [*map-name*]

map-name – Name for the route map. (Range: 1-128 case-sensitive alphanumeric characters)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show route-map RD
route-map RD, permit, sequence 1
Match clauses:
  peer 102.168.0.99
Set clauses:
  comm-list 100 delete
Call clause:
Action:
  Exit routemap
Console#
```


Multicast Routing Commands

Multicast routers can use various kinds of multicast routing protocols to deliver IP multicast packets across different subnetworks. This router supports Protocol Independent Multicasting (PIM). (Note that IGMP will be enabled for any interface that is using multicast routing.)

Table 203: Multicast Routing Commands

Command Group	Function
General Multicast Routing	Enables IP multicast routing globally; also displays the IP multicast routing table created from static and dynamic routing information
Static Multicast Routing	Configures static multicast router ports
PIM Multicast Routing	Configures global and interface settings for PIM-DM and PIM-SM

General Multicast Routing

This section describes commands used to configure multicast routing globally on the switch.

Table 204: General Multicast Routing Commands

Command	Function	Mode
<i>IPv4 Commands</i>		
<code>ip multicast-routing</code>	Enables IPv4 multicast routing	GC
<code>show ip mroute</code>	Shows the IPv4 multicast routing table	PE
<i>IPv6 Commands</i>		
<code>ipv6 multicast-routing</code>	Enables IPv6 multicast routing	GC
<code>show ipv6 mroute</code>	Shows the IPv6 multicast routing table	PE

ip multicast-routing This command enables IPv4 multicast routing. Use the **no** form to disable IP multicast routing.

Syntax

[no] ip multicast-routing

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ This command is used to enable IPv4 multicast routing globally for the router. A specific multicast routing protocol also needs to be enabled on the interfaces that will support multicast routing using the [router pim](#) command, and then specify the interfaces that will support multicast routing using the [ip pim dense-mode](#) or [ip pim sparse-mode](#) commands.
- ◆ To use multicast routing, IGMP proxy can not enabled on any interface of the device (see [ip igmp proxy](#) on [page 681](#)).

Example

```
Console(config)#ip multicast-routing
Console(config)#
```

show ip mroute This command displays the IPv4 multicast routing table.

Syntax

show ip mroute [*group-address source*] [**summary**]

group-address - An IPv4 multicast group address with subscribers directly attached or downstream from this router.

source - The IPv4 subnetwork at the root of the multicast delivery tree. This subnetwork contains a known multicast source.

summary - Displays summary information for each entry in the IP multicast routing table.

Command Mode

Privileged Exec

Command Usage

This command displays information for multicast routing. If no optional parameters are selected, detailed information for each entry in the multicast address table is displayed. If you select a multicast group and source pair, detailed information is displayed only for the specified entry. If the **summary** option is selected, an abbreviated list of information for each entry is displayed on a single line.

Example

This example shows detailed multicast information for a specified group/source pair

```

Console#show ip mroute 224.0.255.3 192.111.46.8

IP Multicast Forwarding is enabled.

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, s - SSM Channel, C - Connected, P - Pruned,
      F - Register flag, R - RPT-bit set, T - SPT-bit set, J - Join SPT
Interface state: F - Forwarding, P - Pruned, L - Local

(192.168.2.1, 224.0.17.17), uptime 00:00:05
Owner: PIM-DM, Flags: D
Incoming Interface: VLAN2, RPF neighbor: 192.168.2.1
Outgoing Interface List:
VLAN1(F)

Console#

```

Table 205: show ip mroute - display description

Field	Description
Flags	<p>The flags associated with this entry:</p> <ul style="list-style-type: none"> ◆ D (Dense) - PIM Dense mode in use. ◆ S (Sparse) - PIM Sparse mode in use. ◆ s (SSM) - A multicast group with the range of IP addresses used for PIM-SSM. ◆ C (Connected) - A member of the multicast group is present on this interface. ◆ P (Pruned) - This route has been terminated. ◆ F (Register flag) - This device is registering for a multicast source. ◆ R (RP-bit set) - The (S,G) entry is pointing to the Rendezvous Point (RP), which normally indicates a pruned state along the shared tree for a particular source. ◆ T (SPT-bit set) - Multicast packets have been received from a source on the shortest path tree. ◆ J (Join SPT) - The rate of traffic arriving over the shared tree has exceeded the SPT-threshold for this group. If the SPT flag is set for (*,G) entries, the next (S,G) packet received will cause the router to join the shortest path tree. If the SPT flag is set for (S,G), the router immediately joins the shortest path tree.
Interface state	The multicast state for the displayed interface.
group address	IP multicast group address for a requested service.
source	Subnetwork containing the IP multicast source.
uptime	The time elapsed since this entry was created.
Owner	The associated multicast protocol (PIM).

Table 205: show ip mroute - display description (Continued)

Field	Description
Incoming Interface	Interface leading to the upstream neighbor. PIM creates a multicast routing tree based on the unicast routing table. If the related unicast routing table does not exist, PIM will still create a multicast routing entry, but displays "Null" for the upstream interface to indicate that the unicast routing table is not valid. This field may also display "Register" to indicate that a pseudo interface is being used to send or receive PIM-SM register packets.
RPF neighbor	IP address of the multicast router immediately upstream for this group.
Outgoing interface list and flags	The interface(s) on which multicast subscribers have been recorded. The flags associated with each interface indicate: <ul style="list-style-type: none">♦ F (Register flag) - This device is registering for a multicast source.♦ P (Pruned) - This route has been terminated.♦ L (Local) - Downstream interface has received IGMP report message from host in this subnet.

This example lists all entries in the multicast table in summary form:

```

Console#show ip mroute summary

IP Multicast Forwarding is enabled

IP Multicast Routing Table (Summary)
Flags: F - Forwarding, P - Pruned

```

Group	Source	Source Mask	Interface	Owner	Flags
224.0.17.17	192.168.2.1	255.255.255.255	VLAN2	PIM-DM	F

```

Total Entry is 1

Console#

```

ipv6 multicast-routing This command enables IPv6 multicast routing. Use the **no** form to disable IP multicast routing.

Syntax

[no] ipv6 multicast-routing

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ♦ This command is used to enable IPv6 multicast routing globally for the router. A multicast routing protocol also needs to be enabled on the interfaces that will support multicast routing using the [router pim6](#) command, and then specify the interfaces that will support multicast routing using the [ipv6 pim](#) command.

- ◆ To use multicast routing, MLD proxy can not enabled on any interface of the device (see [ipv6 mld proxy](#) on [page 692](#)).

Example

```
Console(config)#ipv6 multicast-routing
Console(config)#
```

show ipv6 mroute This command displays the IPv6 multicast routing table.

Syntax

show ipv6 mroute [*group-address source*] [**summary**]

group-address - An IPv6 multicast group address with subscribers directly attached or downstream from this router.

source - The IPv6 subnetwork at the root of the multicast delivery tree. This subnetwork contains a known multicast source.

summary - Displays summary information for each entry in the IP multicast routing table.

Command Mode

Privileged Exec

Command Usage

This command displays information for multicast routing. If no optional parameters are selected, detailed information for each entry in the multicast address table is displayed. If you select a multicast group and source pair, detailed information is displayed only for the specified entry. If the **summary** option is selected, an abbreviated list of information for each entry is displayed on a single line.

Example

This example shows detailed multicast information for a specified group/source pair

```
Console#show ipv6 mroute FF02::0101 FE80::0202

IP Multicast Forwarding is enabled.

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, s - SSM Channel, C - Connected, P - Pruned,
      F - Register flag, R - RPT-bit set, T - SPT-bit set, J - Join SPT
Interface state: F - Forwarding, P - Pruned, L - Local

(FF02::0101, FE80::0202), uptime 00:00:05
Owner: PIM-DM, Flags: D
Incoming Interface: VLAN2, RPF neighbor: FE80::0303
Outgoing Interface List:
VLAN1(F)
Console#
```

Table 206: show ip mroute - display description

Field	Description
Flags	<p>The flags associated with this entry:</p> <ul style="list-style-type: none"> ◆ D (Dense) - PIM Dense mode in use. ◆ S (Sparse) - PIM Sparse mode in use. ◆ s (SSM) - A multicast group with the range of IP addresses used for PIM-SSM. ◆ C (Connected) - A member of the multicast group is present on this interface. ◆ P (Pruned) - This route has been terminated. ◆ F (Register flag) - This device is registering for a multicast source. ◆ R (RP-bit set) - The (S,G) entry is pointing to the Rendezvous Point (RP), which normally indicates a pruned state along the shared tree for a particular source. ◆ T (SPT-bit set) - Multicast packets have been received from a source on the shortest path tree. ◆ J (Join SPT) - The rate of traffic arriving over the shared tree has exceeded the SPT-threshold for this group. If the SPT flag is set for (*,G) entries, the next (S,G) packet received will cause the router to join the shortest path tree. If the SPT flag is set for (S,G), the router immediately joins the shortest path tree.
Interface state	The multicast state for the displayed interface.
group address	IP multicast group address for a requested service.
source	Subnetwork containing the IP multicast source.
Uptime	The time elapsed since this entry was created.
Owner	The associated multicast protocol (PIM).
Incoming Interface	<p>Interface leading to the upstream neighbor.</p> <p>PIM creates a multicast routing tree based on the unicast routing table. If the related unicast routing table does not exist, PIM will still create a multicast routing entry, but displays "Null" for the upstream interface to indicate that the unicast routing table is not valid. This field may also display "Register" to indicate that a pseudo interface is being used to send or receive PIM-SM register packets.</p>
RPF neighbor	IP address of the multicast router immediately upstream for this group.
Outgoing interface list and flags	<p>The interface(s) on which multicast subscribers have been recorded. The flags associated with each interface indicate:</p> <ul style="list-style-type: none"> ◆ F (Register flag) - This device is registering for a multicast source. ◆ P (Pruned) - This route has been terminated. ◆ L (Local) - Downstream interface has received IGMP report message from host in this subnet.

This example lists all entries in the multicast table in summary form:

```

Console#show ipv6 mroute summary

IP Multicast Forwarding is disabled

IP Multicast Routing Table (Summary)
Flags: F - Forwarding, P - Pruned, D - PIM-DM, S - PIM-SM, V - DVMRP,
       M - MLD
Group                                Source                                Interface  Flag
-----
Total Entry is 1
Console#

```

Static Multicast Routing

This section describes commands used to configure static multicast routes on the switch.

Table 207: Static Multicast Routing Commands

Command	Function	Mode
<code>ip igmp snooping vlan mrouter</code>	Adds a multicast router port	GC
<code>show ip igmp snooping mrouter</code>	Shows multicast router ports	PE

ip igmp snooping vlan mrouter This command statically configures a multicast router port. Use the **no** form to remove the configuration.

Syntax

ip igmp snooping vlan *vlan-id* **mrouter** *interface*

no ip igmp snooping vlan *vlan-id* **mrouter** *interface*

vlan-id - VLAN ID (Range: 1-4094)

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-52)

port-channel *channel-id* (Range: 1-8)

Default Setting

No static multicast router ports are configured.

Command Mode

Global Configuration

Command Usage

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to an interface (port or trunk) on your router, you can manually configure that interface to join all the current multicast groups.

Example

The following shows how to configure port 11 as a multicast router port within VLAN 1:

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11
Console(config)#
```

show ip igmp snooping mrouter

This command displays information on statically configured and dynamically learned multicast router ports.

Syntax

show ip igmp snooping mrouter [vlan *vlan-id*]

vlan-id - VLAN ID (Range: 1-4094)

Default Setting

Displays multicast router ports for all configured VLANs.

Command Mode

Privileged Exec

Command Usage

Multicast router port types displayed include Static or Dynamic.

Example

The following shows that port 11 in VLAN 1 is attached to a multicast router:

```
Console#show ip igmp snooping mrouter vlan 1
VLAN M'cast Router Ports Type
-----
  1                Eth 1/11  Static
  2                Eth 1/12  Dynamic
Console#
```

PIM Multicast Routing

This section describes the PIM commands used for IPv4 and IPv6. Note that PIM can run on an IPv4 network and PIM6 on an IPv6 network simultaneously. Also note that Internet Group Management Protocol (IGMP) is used for IPv4 networks and Multicast Listener Discovery (MLD) for IPv6 networks.

Table 208: IPv4 and IPv6 PIM Commands

Command Group	Function
IPv4 PIM Commands	Configures multicast routing for IPv4 PIM.
IPv6 PIM Commands	Configures multicast routing for IPv6 PIM.

IPv4 PIM Commands This section describes commands used to configure IPv4 PIM-DM and PIM-SM dynamic multicast routing on the switch.

Table 209: PIM-DM and PIM-SM Multicast Routing Commands

Command	Function	Mode
<i>Shared Mode Commands</i>		
<code>router pim</code>	Enables IPv4 PIM globally for the router	GC
<code>ip pim</code>	Enables PIM-DM or PIM-SM on the specified interface	IC
<code>ip pim hello-holdtime</code>	Sets the time to wait for hello messages from a neighboring PIM router before declaring it dead	IC
<code>ip pim hello-interval</code>	Sets the interval between sending PIM hello messages	IC
<code>ip pim join-prune-holdtime</code>	Configures the hold time for the prune state	IC
<code>ip pim lan-prune-delay</code>	Informs downstream routers of the delay before it prunes a flow after receiving a prune request	IC
<code>ip pim override-interval</code>	Specifies the time it takes a downstream router to respond to a lan-prune-delay message	IC
<code>ip pim propagation-delay</code>	Configures the propagation delay required for a LAN prune delay message to reach downstream routers	IC
<code>ip pim trigger-hello-delay</code>	Configures the trigger hello delay	IC
<code>show ip pim interface</code>	Displays information about interfaces configured for PIM	NE, PE
<code>show ip pim neighbor</code>	Displays information about PIM neighbors	NE, PE
<i>PIM-DM Commands</i>		
<code>ip pim graft-retry-interval</code>	Configures the time to wait for a Graft acknowledgement before resending a Graft message	IC
<code>ip pim max-graft-retries</code>	Configures the maximum number of times to resend a Graft message if it has not been acknowledged	IC
<code>ip pim state-refresh origination-interval</code>	Sets the interval between PIM-DM state refresh control messages	IC

Table 209: PIM-DM and PIM-SM Multicast Routing Commands (Continued)

Command	Function	Mode
<i>PIM-SM Commands</i>		
<code>ip pim bsr-candidate</code>	Configures the switch as a Bootstrap Router (BSR) candidate	GC
<code>ip pim register-rate-limit</code>	Configures the rate at which register messages are sent by the Designated Router (DR)	GC
<code>ip pim register-source</code>	Configure the IP source address of a register message to an address other than the outgoing interface address of the designated router (DR) leading toward the rendezvous point (RP)	GC
<code>ip pim rp-address</code>	Sets a static address for the rendezvous point	GC
<code>ip pim rp-candidate</code>	Configures the switch rendezvous point (RP) candidate	GC
<code>ip pim spt-threshold</code>	Prevents the last-hop PIM router from switching to Shortest Path Source Tree (SPT) mode	GC
<code>ip pim dr-priority</code>	Sets the priority value for a DR candidate	IC
<code>ip pim join-prune-interval</code>	Sets the join/prune timer	IC
<code>clear ip pim bsr rp-set</code>	Clears RP entries learned through the BSR	PE
<code>show ip pim bsr-router</code>	Displays information about the BSR	PE
<code>show ip pim rp mapping</code>	Displays active RPs and associated multicast routing entries	PE
<code>show ip pim rp-hash</code>	Displays the RP used for the specified multicast group	PE

PIM Shared Mode Commands

router pim This command enables IPv4 Protocol-Independent Multicast routing globally on the router. Use the **no** form to disable PIM multicast routing.

Syntax

[no] router pim

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ This command enables PIM-DM and PIM-SM globally for the router. You also need to enable PIM-DM or PIM-SM for each interface that will support multicast routing using the `ip pim dense-mode` or `ip pim sparse mode` command, and make any changes necessary to the multicast protocol parameters.
- ◆ To use multicast routing, IGMP proxy cannot be enabled on any interface of the device (see the `ip igmp proxy` command).

Example

```

Console(config)#router pim
Console(config)#exit
Console#show ip pim interface
PIM is enabled.
VLAN 1 is up.
PIM Mode           :      Dense Mode
IP Address          :      192.168.0.2
Hello Interval      :      30 sec
Hello HoldTime      :      105 sec
Triggered Hello Delay :      5 sec
Join/Prune Holdtime :      210 sec
Lan Prune Delay     :      Disabled
Propagation Delay    :      500 ms
Override Interval    :      2500 ms
Graft Retry Interval :      3 sec
Max Graft Retries    :      3
State Refresh Ori Int :      60 sec

Console#

```

ip pim This command enables PIM-DM or PIM-SM on the specified interface. Use the **no** form to disable PIM-DM or PIM-SM on this interface.

Syntax

[no] ip pim {dense-mode | sparse-mode}

dense-mode - Enables PIM Dense Mode.

sparse-mode - Enables PIM Sparse Mode.

Default Setting

Disabled

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ To fully enable PIM, you need to enable multicast routing globally for the router with the [ip multicast-routing](#) command, enable PIM globally for the router with the [router pim](#) command, and also enable PIM-DM or PIM-SM for each interface that will participate in multicast routing with this command.
- ◆ If you enable PIM on an interface, you should also enable IGMP on that interface. PIM mode selection determines how the switch populates the multicast routing table, and how it forwards packets received from directly connected LAN interfaces. Dense mode interfaces are always added to the multicast routing table. Sparse mode interfaces are added only when periodic join messages are received from downstream routers, or a group member is directly connected to the interface.

- ◆ Dense-mode interfaces are subject to multicast flooding by default, and are only removed from the multicast routing table when the router determines that there are no group members or downstream routers, or when a prune message is received from a downstream router.
- ◆ Sparse-mode interfaces forward multicast traffic only if a join message is received from a downstream router or if group members are directly connected to the interface. When routers want to receive a multicast flow, they periodically send join messages to the Rendezvous Point (RP), and are subsequently added to the shared path for the specified flow back up to the RP. If routers want to join the source path up through the Shortest Path Source Tree (SPT), they periodically send join messages toward the source. They also send prune messages toward the RP to prune the shared path if they have already connected to the source through the SPT, or if there are no longer any group members connected to the interface.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip pim dense-mode
Console(config-if)#end
Console#show ip pim interface
PIM is enabled.
VLAN 1 is up.
PIM Mode                :      Dense Mode
IP Address                :      192.168.0.2
Hello Interval           :      30 sec
Hello HoldTime           :      105 sec
Triggered Hello Delay    :      5 sec
Join/Prune Holdtime      :      210 sec
Lan Prune Delay          :      Disabled
Propagation Delay        :      500 ms
Override Interval        :      2500 ms
Graft Retry Interval     :      3 sec
Max Graft Retries        :      3
State Refresh Ori Int    :      60 sec

Console#
```

ip pim hello-holdtime This command configures the interval to wait for hello messages from a neighboring PIM router before declaring it dead. Use the **no** form to restore the default value.

Syntax

ip pim hello-holdtime *seconds*

no ip pim hello-interval

seconds - The hold time for PIM hello messages. (Range: 1-65535)

Default Setting

105 seconds

Command Mode

Interface Configuration (VLAN)

Command Usage

The **ip pim hello-holdtime** should be greater than the value of **ip pim hello-interval**.

Example

```
Console(config-if)#ip pim hello-holdtime 210
Console(config-if)#
```

ip pim hello-interval This command configures the frequency at which PIM hello messages are transmitted. Use the **no** form to restore the default value.

Syntax**ip pim hello-interval** *seconds***no pim hello-interval***seconds* - Interval between sending PIM hello messages. (Range: 1-65535)**Default Setting**

30 seconds

Command Mode

Interface Configuration (VLAN)

Command Usage

Hello messages are sent to neighboring PIM routers from which this device has received probes, and are used to verify whether or not these neighbors are still active members of the multicast tree.

Example

```
Console(config-if)#ip pim hello-interval 60
Console(config-if)#
```

ip pim join-prune-holdtime This command configures the hold time for the prune state. Use the **no** form to restore the default value.

Syntax**ip pim join-prune-holdtime** *seconds***no ip pim join-prune-holdtime***seconds* - The hold time for the prune state. (Range: 0-65535)

Default Setting

210 seconds

Command Mode

Interface Configuration (VLAN)

Command Usage

The multicast interface that first receives a multicast stream from a particular source forwards this traffic to all other PIM interfaces on the router. If there are no requesting groups on that interface, the leaf node sends a prune message upstream and enters a prune state for this multicast stream. The prune state is maintained until the join-prune-holdtime timer expires or a graft message is received for the forwarding entry.

Example

```
Console(config-if)#ip pim join-prune-holdtime 60
Console(config-if)#
```

ip pim lan-prune-delay

This command causes this device to inform downstream routers of how long it will wait before pruning a flow after receiving a prune request. Use the **no** form to disable this feature.

Syntax

[no] ip pim lan-prune-delay

Default Setting

Disabled

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ When other downstream routers on the same VLAN are notified that this upstream router has received a prune request, they must send a Join to override the prune before the prune delay expires if they want to continue receiving the flow. The message generated by this command effectively prompts any downstream neighbors with hosts receiving the flow to reply with a Join message. If no join messages are received after the prune delay expires, this router will prune the flow.
- ◆ Prune delay is the sum of the effective propagation-delay and effective override-interval, where effective propagation-delay is the largest propagation-delay from those advertised by each neighbor (including this switch), and effective override-interval is the largest override-interval from those advertised by each neighbor (including this switch).

Example

```
Console(config-if)#ip pim lan-prune-delay  
Console(config-if)#
```

Related Commands

[ip pim override-interval \(1025\)](#)

[ip pim propagation-delay \(1026\)](#)

ip pim override-interval This command configures the override interval, or the time it takes a downstream router to respond to a lan-prune-delay message. Use the **no** form to restore the default setting.

Syntax

ip pim override-interval *milliseconds*

no ip pim override-interval

milliseconds - The time required for a downstream router to respond to a lan-prune-delay message by sending back a Join message if it wants to continue receiving the flow referenced in the message. (Range: 500-6000 milliseconds)

Default Setting

2500 milliseconds

Command Mode

Interface Configuration (VLAN)

Command Usage

The override interval configured by this command and the propagation delay configured by the [ip pim propagation-delay](#) command are used to calculate the LAN prune delay. If a downstream router has group members which want to continue receiving the flow referenced in a LAN prune delay message, then the override interval represents the time required for the downstream router to process the message and then respond by sending a Join message back to the upstream router to ensure that the flow is not terminated.

Example

```
Console(config-if)#ip pim override-interval 3500  
Console(config-if)#
```

Related Commands

[ip pim propagation-delay \(1026\)](#)

[ip pim lan-prune-delay \(1024\)](#)

ip pim propagation-delay This command configures the propagation delay required for a LAN prune delay message to reach downstream routers. Use the **no** form to restore the default setting.

ip pim propagation-delay *milliseconds*

no ip pim propagation-delay

milliseconds - The time required for a lan-prune-delay message to reach downstream routers attached to the same VLAN interface. (Range: 100-5000 milliseconds)

Default Setting

500 milliseconds

Command Mode

Interface Configuration (VLAN)

Command Usage

The override interval configured by the [ip pim override-interval](#) command and the propagation delay configured by this command are used to calculate the LAN prune delay. If a downstream router has group members which want to continue receiving the flow referenced in a LAN prune delay message, then the propagation delay represents the time required for the lan-prune-delay message to be propagated down from the upstream router to all downstream routers attached to the same VLAN interface.

Example

```
Console(config-if)#ip pim propagation-delay 600
Console(config-if)#
```

Related Commands

[ip pim override-interval \(1025\)](#)

[ip pim lan-prune-delay \(1024\)](#)

ip pim trigger-hello-delay This command configures the maximum time before transmitting a triggered PIM Hello message after the router is rebooted or PIM is enabled on an interface. Use the **no** form to restore the default value.

Syntax

ip pim trigger-hello-delay *seconds*

no ip pim trigger-hello-delay

seconds - The maximum time before sending a triggered PIM Hello message. (Range: 0-5 seconds)

Default Setting

5 seconds

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ When a router first starts or PIM is enabled on an interface, the hello delay is set to random value between 0 and the trigger-hello-delay. This prevents synchronization of Hello messages on multi-access links if multiple routers are powered on simultaneously.
- ◆ Also, if a Hello message is received from a new neighbor, the receiving router will send its own Hello message after a random delay between 0 and the trigger-hello-delay.

Example

```
Console(config-if)#ip pim trigger-hello-delay 3
Console(config-if)#
```

show ip pim interface This command displays information about interfaces configured for PIM.

Syntax

show ip pim interface [vlan *vlan-id*]

vlan-id - VLAN ID (Range: 1-4094)

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command displays the PIM settings for the specified interface as described in the preceding pages. It also shows the address of the designated PIM router and the number of neighboring PIM routers.

Example

```
Console#show ip pim interface vlan 1
PIM is enabled.
VLAN 1 is up.
PIM Mode           :      Dense Mode
IP Address          :      192.168.0.2
Hello Interval      :      30 sec
Hello HoldTime      :      105 sec
Triggered Hello Delay :      5 sec
Join/Prune Holdtime :      210 sec
Lan Prune Delay     :      Disabled
Propagation Delay    :      500 ms
Override Interval    :      2500 ms
Graft Retry Interval :      3 sec
Max Graft Retries    :      3
State Refresh Ori Int :      60 sec
```

Console#

show ip pim neighbor This command displays information about PIM neighbors.

Syntax

show ip pim neighbor [**interface vlan** *vlan-id*]

vlan-id - VLAN ID (Range: 1-4094)

Default Setting

Displays information for all known PIM neighbors.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show ip pim neighbor
Neighbor Address VLAN Interface Uptime (sec.) Expiration Time (sec) DR
-----
192.168.0.3/32 1 00:00:21 00:01:30
Console#
```

Table 210: show ip pim neighbor - display description

Field	Description
Neighbor Address	IP address of the next-hop router.
VLAN Interface	Interface number that is attached to this neighbor.
Uptime	The duration this entry has been active.
Expiration Time	The time before this entry will be removed.
DR	The designated PIM-SM router. If multicast hosts are directly connected to the LAN, then only one of these routers is elected as the DR, and acts on behalf of these hosts, sending periodic Join/Prune messages toward a group-specific RP for each group.

PIM-DM Commands

ip pim graft-retry-interval This command configures the time to wait for a Graft acknowledgement before resending a Graft. Use the **no** form to restore the default value.

Syntax

ip pim graft-retry-interval *seconds*

no ip pim graft-retry-interval

seconds - The time before resending a Graft. (Range: 1-10 seconds)

Default Setting

3 seconds

Command Mode

Interface Configuration (VLAN)

Command Usage

A graft message is sent by a router to cancel a prune state. When a router receives a graft message, it must respond with an graft acknowledgement message. If this acknowledgement message is lost, the router that sent the graft message will resend it a number of times (as defined by the `ip pim max-graft-retries` command).

Example

```
Console(config-if)#ip pim graft-retry-interval 9
Console(config-if)#
```

ip pim max-graft-retries

This command configures the maximum number of times to resend a Graft message if it has not been acknowledged. Use the **no** form to restore the default value.

Syntax

ip pim max-graft-retries *retries*

no ip pim max-graft-retries

retries - The maximum number of times to resend a Graft. (Range: 1-10)

Default Setting

3

Command Mode

Interface Configuration (VLAN)

Example

```
Console(config-if)#ip pim max-graft-retries 5
Console(config-if)#
```

ip pim state-refresh origination-interval

This command sets the interval between sending PIM-DM state refresh control messages. Use the **no** form to restore the default value.

Syntax

ip pim state-refresh origination-interval *seconds*

no ip pim max-graft-retries

seconds - The interval between sending PIM-DM state refresh control messages. (Range: 1-100 seconds)

Default Setting

60 seconds

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ The pruned state times out approximately every three minutes and the entire PIM-DM network is reflooded with multicast packets and prune messages. The state refresh feature keeps the pruned state from timing out by periodically forwarding a control message down the distribution tree, refreshing the prune state on the outgoing interfaces of each router in the tree. This also enables PIM routers to recognize topology changes (sources joining or leaving a multicast group) before the default three-minute state timeout expires.
- ◆ This command is only effectively for interfaces of first hop, PIM-DM routers that are directly connected to the sources of multicast groups.

Example

```
Console(config-if)#ip pim state-refresh origination-interval 30
Console(config-if)#
```

PIM-SM Commands

ip pim bsr-candidate This command configures the switch as a Bootstrap Router (BSR) candidate. Use the **no** form to restore the default value.

Syntax

**ip pim bsr-candidate interface vlan *vlan-id* [*hash hash-mask-length*]
[*priority priority*]**

no ip pim bsr-candidate

vlan-id - VLAN ID (Range: 1-4094)

hash-mask-length - Hash mask length (in bits) used for RP selection (see [ip pim rp-candidate](#) and [ip pim rp-address](#)). The portion of the hash specified by the mask length is ANDed with the group address. Therefore, when the hash function is executed on any BSR, all groups with the same seed hash will be mapped to the same RP. If the mask length is less than 32, then only the first portion of the hash is used, and a single RP will be defined for multiple groups. (Range: 0-32 bits)

priority - Priority used by the candidate bootstrap router in the election process. The BSR candidate with the largest priority is preferred. If the priority values are the same, the candidate with the larger IP address is elected to be the BSR. Setting the priority to zero means that this router is not eligible to server as the BSR. At least one router in the PIM-SM domain must be set to a value greater than zero. (Range: 0-255)

Default Setting

Hash Mask Length: 10

Priority: 0

Command Mode

Global Configuration

Command Usage

- ◆ When the **ip pim bsr-candidate** command is entered, the router starts sending bootstrap messages to all of its PIM-SM neighbors. The IP address of the designated VLAN is sent as the candidate's BSR address. Each neighbor receiving the bootstrap message compares the BSR address with the address from previous messages. If the current address is the same or a higher address, it accepts the bootstrap message and forwards it. Otherwise, it drops the message.
- ◆ This router will continue to be the BSR until it receives a bootstrap message from another candidate with a higher priority (or a higher IP address if the priorities are the same).
- ◆ To improve failover recovery, it is advisable to select at least two core routers in diverse locations, each to serve as both a candidate BSR and candidate RP. It is also preferable to set up one of these routers as both the primary BSR and RP.

Example

The following example configures the router to start sending bootstrap messages out of the interface for VLAN 1 to all of its PIM-SM neighbors.

```
Console(config)#ip pim bsr-candidate interface vlan 1 hash 20 priority 200
Console(config)#exit
Console#show ip pim bsr-router
PIMv2 Bootstrap information
BSR Address       : 192.168.0.2/32
Uptime           : 00:00:08
BSR Priority      : 200
Hash Mask Length : 20
Expire            : 00:00:57
Role              : Candidate BSR
State            : Elected BSR
Console#
```

ip pim register-rate-limit This command configures the rate at which register messages are sent by the Designated Router (DR) for each (source, group) entry. Use the **no** form to restore the default value.

Syntax

ip pim register-rate-limit *rate*

no ip pim register-rate-limit

rate - The maximum number of register packets per second. (Range: 1-65535; Default: 0, which means no limit)

Default Setting

0

Command Mode

Global Configuration

Command Usage

This command can be used to relieve the load on the Designated Router (DR) and RP. However, because register messages exceeding the limit are dropped, some receivers may experience data packet loss within the first few seconds in which register messages are sent from bursty sources.

Example

This example sets the register rate limit to 500 pps.

```
Console(config)#ip pim register-rate-limit 500
Console(config)#
```

ip pim register-source This command configures the IP source address of a register message to an address other than the outgoing interface address of the designated router (DR) that leads back toward the rendezvous point (RP). Use the **no** form to restore the default setting.

Syntax

ip pim register-source interface vlan *vlan-id*

no ip pim register-source

vlan-id - VLAN ID (Range: 1-4094)

Default Setting

The IP address of the DR's outgoing interface that leads back to the RP

Command Mode

Global Configuration

Command Usage

When the source address of a register message is filtered by intermediate network devices, or is not a uniquely routed address to which the RP can send packets, the replies sent from the RP to the source address will fail to reach the DR, resulting in PIM-SM protocol failures. This command can be used to overcome this type of problem by manually configuring the source address of register messages to an interface that leads back to the RP.

Example

This example sets the register rate limit to 500 pps.

```
Console(config)#ip pim register-source interface vlan 1
Console(config)#
```

ip pim rp-address This command sets a static address for the Rendezvous Point (RP) for a particular multicast group. Use the **no** form to remove an RP address or an RP address for a specific group.

Syntax

[no] ip pim rp-address *rp-address* [**group-prefix** *group-address mask*]

rp-address - Static IP address of the router that will be an RP for the specified multicast group(s).

group-address - An IP multicast group address. If a group address is not specified, the RP is used for all multicast groups.

mask - Subnet mask that is used for the group address.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ The router specified by this command will act as an RP for all multicast groups in the local PIM-SM domain if no groups are specified. A static RP can either be configured for the whole multicast group range 224.0.0.0/4, or for specific group ranges.
- ◆ Using this command to configure multiple static RPs with the same RP address is not allowed. If an IP address is specified that was previously used for an RP, then the older entry is replaced.
- ◆ Multiple RPs can be defined for different groups or group ranges. If a group is matched by more than one entry, the router will use the RP associated with the

longer group prefix length. If the prefix lengths are the same, then the static RP with the highest IP address is chosen.

- ◆ Static definitions for RP addresses may be used together with RP addresses dynamically learned through the bootstrap router (BSR). If an RP address learned by the BSR and one statically configured using this command are both available for a group range, the RP address learned by the BSR is chosen over the one statically configured with this command.
- ◆ All routers within the same PIM-SM domain must be configured with the same RP(s). Selecting an RP through the dynamic election process is therefore preferable for most situations. Using the dynamic RP election process also allows a backup RP to automatically take over if the active RP router becomes unavailable.
- ◆ If the **no** form of this command is used without specifying a multicast group, the default 224.0.0.0 (with the mask 240.0.0.0) is removed. In other words, all multicast groups are removed.

Example

In the following example, the first PIM-SM command just specifies the RP address 192.168.1.1 to indicate that it will be used to service all multicast groups. The second PIM-SM command includes the multicast groups to be serviced by the RP.

```
Console(config)#ip pim rp-address 192.168.1.1
Console(config)#ip pim rp-address 192.168.2.1 group-prefix 224.9.0.0
255.255.0.0
Console(config)#end
Console#show ip pim rp mapping
PIM Group-to-RP Mappings
Groups          : 224.0.0.0/4
RP address      : 192.168.1.1/32
Info source     : static
Uptime         : 00:00:33
Expire         : Never
Groups          : 224.9.0.0/16
RP address      : 192.168.2.1/32
Info source     : static
Uptime         : 00:00:21
Expire         : Never
Console#
```

ip pim rp-candidate This command configures the router to advertise itself as a Rendezvous Point (RP) candidate to the bootstrap router (BSR). Use the **no** form to remove this router as an RP candidate.

Syntax

**ip pim rp-candidate interface vlan *vlan-id* [*group-prefix group-address mask*]
[*interval seconds*] [*priority value*]**

no ip pim rp-candidate interface vlan *vlan-id*

vlan-id - VLAN ID (Range: 1-4094)

group-address - An IP multicast group address. If a group address is not specified, the RP is advertised for all multicast groups.

mask - Subnet mask that is used for the group address.

seconds - The interval at which this device advertises itself as an RP candidate. (Range: 60-16383 seconds)

value - Priority used by the candidate RP in the election process. The RP candidate with the largest priority is preferred. If the priority values are the same, the candidate with the larger IP address is elected to be the RP. Setting the priority to zero means that this router is not eligible to server as the RP. (Range: 0-255)

Default Setting

Address: 224.0.0.0/4, or the entire IPv4 multicast group family

Interval: 60 seconds

Priority: 0

Command Mode

Global Configuration

Command Usage

- ◆ When the **ip pim rp-candidate** command is entered, the router periodically sends PIMv2 messages to the BSR advertising itself as a candidate RP for the specified group addresses. The IP address of the designated VLAN is sent as the candidate's RP address. The BSR places information about all of the candidate RPs in subsequent bootstrap messages. The BSR uses the RP-election hash algorithm to select an active RP for each group range. The election process is performed by the BSR only for its own use. Each PIM-SM router that receives the list of RP candidates from the BSR also elects an active RP for each group range using the same election process.
- ◆ The election process for each group is based on the following criteria:
 - Find all RPs with the most specific group range.
 - Select those with the highest priority (lowest priority value).

- Compute a hash value based on the group address, RP address, priority, and hash mask included in the bootstrap messages.
- If there is a tie, use the candidate RP with the highest IP address.
- ◆ This distributed election process provides faster convergence and minimal disruption when an RP fails. It also serves to provide load balancing by distributing groups across multiple RPs. Moreover, when an RP fails, the responsible RPs are re-elected on each router, and the groups automatically distributed to the remaining RPs.
- ◆ To improve failover recovery, it is advisable to select at least two core routers in diverse locations, each to serve as both a candidate BSR and candidate RP. It is also preferable to set up one of these routers as both the primary BSR and RP.

Example

The following example configures the router to start advertising itself to the BSR as a candidate RP for the indicated multicast groups.

```
Console(config)#ip pim rp-candidate interface vlan 1 group-prefix 224.0.0.0
255.0.0.0
Console(config)#end
Console#show ip pim rp mapping
PIM Group-to-RP Mappings
Groups          : 224.0.0.0/8
RP address      : 192.168.0.2/32
Info source     : 192.168.0.2/32, via bootstrap, priority: 0
Uptime         : 00:00:51
Expire         : 00:01:39
Console#
```

ip pim spt-threshold This command prevents the last-hop PIM router from switching to Shortest Path Source Tree (SPT) mode. Use the **no** form to allow the router to switch over to SPT mode.

Syntax

ip pim spt-threshold infinity [**group-prefix** *group-address* *mask*]

no ip pim spt-threshold infinity

group-address - An IP multicast group address. If a group address is not specified, the command applies to all multicast groups.

mask - Subnet mask that is used for the group address.

Default Setting

The last-hop PIM router joins the shortest path tree immediately after the first packet arrives from a new source.

Command Mode

Global Configuration

Command Usage

- ◆ The default path for packets from a multicast source to a receiver is through the RP. However, the path through the RP is not always the shortest path. Therefore, the router uses the RP to forward only the first packet from a new multicast group to its receivers. Afterwards, it calculates the shortest path tree (SPT) directly between the receiver and source, and then uses the SPT to send all subsequent packets from the source to the receiver instead of using the shared tree. Note that when the SPT threshold is not set by this command, the PIM leaf router will join the shortest path tree immediately after receiving the first packet from a new source.
- ◆ This command forces the router to use the shared tree for all multicast groups, or just for the specified multicast groups.
- ◆ Only one entry is allowed for this command.

Example

This example prevents the switch from using the SPT for multicast groups 224.1.0.0~224.1.255.255.

```
Console(config)#ip pim spt-threshold infinity group-prefix 224.1.0.0
0.0.255.255
Console#
```

ip pim dr-priority This command sets the priority value for a Designated Router (DR) candidate. Use the **no** form to restore the default setting.

Syntax

ip pim dr-priority *priority-value*

no ip pim dr-priority

priority-value - Priority advertised by a router when bidding to become the DR. (Range: 0-4294967294)

Default Setting

1

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ More than one PIM-SM router may be connected to an Ethernet or other shared-media LAN. If multicast hosts are directly connected to the LAN, then only one of these routers is elected as the DR, and acts on behalf of these hosts, sending periodic Join/Prune messages toward a group-specific RP for each group. A single DR is elected per interface (LAN or otherwise) using a simple election process.

- ◆ The router with the highest priority configured on an interface is elected as the DR. If more than one router attached to this interface uses the same priority, then the router with the highest IP address is elected to serve as the DR.
- ◆ If a router does not advertise a priority in its hello messages, it is assumed to have the highest priority and is elected as the DR. If more than one router is not advertising its priority, then the router with the highest IP address is elected to serve as the DR.

Example

This example sets the priority used in the bidding process for the DR.

```
Console(config)#interface vlan 1
Console(config-if)#ip pim dr-priority 20
Console(config-if)#end
Console#show ip pim interface
PIM is enabled.
VLAN 1 is up.
PIM Mode           : Sparse Mode
IP Address          : 192.168.0.2
Hello Interval      : 30 sec
Hello HoldTime      : 105 sec
Triggered Hello Delay : 5 sec
Join/Prune Holdtime : 210 sec
Lan Prune Delay     : Disabled
Propagation Delay    : 500 ms
Override Interval    : 2500 ms
DR Priority          : 20
Join/Prune Interval  : 60 sec

Console#
```

ip pim join-prune-interval This command sets the join/prune timer. Use the **no** form to restore the default setting.

Syntax

ip pim join-prune-interval *seconds*

no ip pim join-prune-interval

seconds - The interval at which join/prune messages are sent. (Range: 1-65535 seconds)

Default Setting

60 seconds

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ By default, the switch sends join/prune messages every 210 seconds to inform other PIM-SM routers about clients who want to join or leave a multicast group.

- ◆ Use the same join/prune message interval on all the PIM-SM routers in the same PIM-SM domain, otherwise the routing protocol's performance will be adversely affected.
- ◆ The multicast interface that first receives a multicast stream from a particular source forwards this traffic only to those interfaces on the router that have requested to join this group. When there are no longer any requesting groups on that interface, the leaf node sends a prune message upstream and enters a prune state for this multicast stream. The protocol maintains both the current join state and the pending Reverse Path Tree (RPT) prune state for this (source, group) pair until the join/prune-interval timer expires.

Example

This example sets the priority used in the bidding process for the DR.

```

Console(config)#interface vlan 1
Console(config-if)#ip pim join-prune-interval 210
Console#show ip pim interface
PIM is enabled.
VLAN 1 is up.
PIM Mode           :      Sparse Mode
IP Address          :      192.168.0.2
Hello Interval      :      30 sec
Hello HoldTime      :      105 sec
Triggered Hello Delay :      5 sec
Join/Prune Holdtime :      210 sec
Lan Prune Delay      :      Disabled
Propagation Delay    :      500 ms
Override Interval    :      2500 ms
DR Priority           :      20
Join/Prune Interval  :      80 sec

Console#

```

clear ip pim bsr rp-set This command clears multicast group to RP mapping entries learned through the PIMv2 bootstrap router (BSR).

Command Mode

Privileged Exec

Command Usage

- ◆ This command can be used to update entries in the static multicast forwarding table immediately after making configuration changes to the RP.
- ◆ Use the [show ip pim rp mapping](#) command to display active RPs that are cached with associated multicast routing entries.

Example

This example clears the RP map.

```
Console#clear ip pim bsr rp-set
Console#show ip pim rp mapping
PIM Group-to-RP Mappings
Console#
```

show ip pim bsr-router This command displays information about the bootstrap router (BSR).

Command Mode

Privileged Exec

Command Usage

This command displays information about the elected BSR.

Example

This example displays information about the BSR.

```
Console#show ip pim bsr-router
PIMv2 Bootstrap information
BSR Address      : 192.168.0.2/32
Uptime          : 01:01:23
BSR Priority     : 200
Hash Mask Length : 20
Expire          : 00:00:42
Role            : Candidate BSR
State           : Elected BSR
Console#
```

Table 211: show ip pim bsr-router - display description

Field	Description
BSR Address	IP address of interface configured as the BSR.
Uptime	The time this BSR has been up and running.
BSR Priority	Priority assigned to this interface for use in the BSR election process.
Hash Mask Length	The number of significant bits used in the multicast group comparison mask. This mask determines the multicast group for which this router can be a BSR.
Expire	The time before this entry will be removed.
Role	Candidate BSR or Non-candidate BSR.

Table 211: show ip pim bsr-router - display description

Field	Description
State	<p>Operation state of BSR includes:</p> <ul style="list-style-type: none"> ◆ No information – No information stored for this device. ◆ Accept Any – The router does not know of an active BSR, and will accept the first bootstrap message it sees as giving the new BSR's identity and the RP-set. ◆ Accept Preferred – The router knows the identity of the current BSR, and is using the RP-set provided by that BSR. Only bootstrap messages from that BSR or from a C-BSR with higher weight than the current BSR will be accepted. ◆ Candidate BSR – Bidding in election process. ◆ Pending-BSR – The router is a candidate to be the BSR for the RP-set. Currently, no other router is the preferred BSR, but this router is not yet the elected BSR. ◆ Elected BSR – elected to serve as BSR

show ip pim rp mapping This command displays active RPs and associated multicast routing entries.

Command Mode
Privileged Exec

Example
This example displays the RP map.

```

Console#show ip pim rp mapping
PIM Group-to-RP Mappings
Groups          : 224.0.0.0/8
RP address      : 192.168.0.2/32
Info source     : 192.168.0.2/32, via bootstrap, priority: 0
Uptime         : 00:31:09
Expire          : 00:02:21

Console#

```

Table 212: show ip pim rp mapping - display description

Field	Description
Groups	The multicast group address, mask length managed by the RP.
RP address	IP address of the RP used for the listed multicast group
Info source	RP that advertised the mapping, how the RP was selected (Static or Bootstrap), and the priority used in the bidding process
Uptime	The time this RP has been up and running
Expire	The time before this entry will be removed

show ip pim rp-hash This command displays the RP used for the specified multicast group, and the RP that advertised the mapping.

Syntax

show ip pim rp-hash *group-address*

group-address - An IP multicast group address.

Command Mode

Privileged Exec

Example

This example displays the RP used for the specified group.

```
Console#show ip pim rp-hash 224.0.1.3
RP address      : 192.168.0.2/32
Info source     : 192.168.0.2/32, via (null)
Console#
```

Table 213: show ip pim rp-hash - display description

Field	Description
RP address	IP address of the RP used for the specified multicast group
Info source	RP that advertised the mapping, and how the RP was selected

IPv6 PIM Commands This section describes commands used to configure IPv6 PIM dynamic multicast routing on the switch.

Table 214: PIM-DM and PIM-SM Multicast Routing Commands

Command	Function	Mode
<i>Shared Mode Commands</i>		
router pim6	Enables IPv6 PIM globally for the router	GC
ipv6 pim	Enables PIM-DM or PIM-SM on the specified interface	IC
ipv6 pim hello-holdtime	Sets the time to wait for hello messages from a neighboring PIM router before declaring it dead	IC
ipv6 pim hello-interval	Sets the interval between sending PIM hello messages	IC
ipv6 pim join-prune-holdtime	Configures the hold time for the prune state	IC
ipv6 pim lan-prune-delay	Informs downstream routers of the delay before it prunes a flow after receiving a prune request	IC
ipv6 pim override-interval	Specifies the time it takes a downstream router to respond to a lan-prune-delay message	IC
ipv6 pim propagation-delay	Configures the propagation delay required for a LAN prune message to reach downstream routers	IC

Table 214: PIM-DM and PIM-SM Multicast Routing Commands (Continued)

Command	Function	Mode
<code>ipv6 pim trigger-hello-delay</code>	Configures the trigger hello delay	IC
<code>show ipv6 pim interface</code>	Displays information about interfaces configured for PIM	NE, PE
<code>show ipv6 pim neighbor</code>	Displays information about PIM neighbors	NE, PE
<i>PIM-DM Commands</i>		
<code>ipv6 pim graft-retry-interval</code>	Configures the time to wait for a Graft acknowledgement before resending a Graft message	IC
<code>ipv6 pim max-graft-retries</code>	Configures the maximum number of times to resend a Graft message if it has not been acknowledged	IC
<code>ipv6 pim state-refresh origination-interval</code>	Sets the interval between PIM-DM state refresh control messages	IC
<i>PIM-SM Commands</i>		
<code>ipv6 pim bsr-candidate</code>	Configures the switch as a Bootstrap Router (BSR) candidate	GC
<code>ipv6 pim register-rate-limit</code>	Configures the rate at which register messages are sent by the Designated Router (DR)	GC
<code>ipv6 pim register-source</code>	Configure the IP source address of a register message to an address other than the outgoing interface address of the designated router (DR) leading toward the rendezvous point (RP)	GC
<code>ipv6 pim rp-address</code>	Sets a static address for the rendezvous point	GC
<code>ipv6 pim rp-candidate</code>	Configures the switch rendezvous point (RP) candidate	GC
<code>ipv6 pim spt-threshold</code>	Prevents the last-hop PIM router from switching to Shortest Path Source Tree (SPT) mode	GC
<code>ipv6 pim dr-priority</code>	Sets the priority value for a DR candidate	IC
<code>ipv6 pim join-prune-interval</code>	Sets the join/prune timer	IC
<code>clear ipv6 pim bsr rp-set</code>	Clears RP entries learned through the BSR	PE
<code>show ipv6 pim bsr-router</code>	Displays information about the BSR	PE
<code>show ipv6 pim rp mapping</code>	Displays active RPs and associated multicast routing entries	PE
<code>show ipv6 pim rp-hash</code>	Displays the RP used for the specified multicast group	PE

PIM6 Shared Mode Commands

router pim6 This command enables IPv6 Protocol-Independent Multicast routing globally on the router. Use the **no** form to disable PIM multicast routing.

Syntax

[no] router pim6

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ This command enables PIM-DM and PIM-SM for IPv6 globally for the router. You also need to enable PIM-DM and PIM-SM for each interface that will support multicast routing using the [ipv6 pim](#) command, and make any changes necessary to the multicast protocol parameters.
- ◆ To use PIMv6, IPv6 multicast routing must be enabled on the switch using the [ipv6 multicast-routing](#) command.
- ◆ To use IPv6 multicast routing, MLD proxy cannot be enabled on any interface of the device (see the [ipv6 mld proxy](#) command).

Example

```
Console(config)#router pim6
Console(config)#
```

ipv6 pim This command enables IPv6 PIM-DM or PIM-SM on the specified interface. Use the **no** form to disable IPv6 PIM-DM or PIM-SM on this interface.

Syntax

[no] ipv6 pim {dense-mode | sparse-mode}

dense-mode - Enables PIM Dense Mode.

sparse-mode - Enables PIM Sparse Mode.

Default Setting

Disabled

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ To fully enable PIM, you need to enable multicast routing globally for the router with the [ipv6 multicast-routing](#) command, enable PIM globally for the router with the [router pim6](#) command, and also enable PIM-DM or PIM-SM for each interface that will participate in multicast routing with this command.
- ◆ If you enable PIM on an interface, you should also enable MLD (see [“MLD \(Layer 3\)” on page 683](#)) on that interface. PIM mode selection determines how the switch populates the multicast routing table, and how it forwards packets received from directly connected LAN interfaces. Dense mode interfaces are always added to the multicast routing table. Sparse mode interfaces are added only when periodic join messages are received from downstream routers, or a group member is directly connected to the interface.

- ◆ Dense-mode interfaces are subject to multicast flooding by default, and are only removed from the multicast routing table when the router determines that there are no group members or downstream routers, or when a prune message is received from a downstream router.
- ◆ Sparse-mode interfaces forward multicast traffic only if a join message is received from a downstream router or if group members are directly connected to the interface. When routers want to receive a multicast flow, they periodically send join messages to the Rendezvous Point (RP), and are subsequently added to the shared path for the specified flow back up to the RP. If routers want to join the source path up through the Shortest Path Source Tree (SPT), they periodically send join messages toward the source. They also send prune messages toward the RP to prune the shared path if they have already connected to the source through the SPT, or if there are no longer any group members connected to the interface.

Example

```

Console(config)#interface vlan 1
Console(config-if)#ipv6 pim dense-mode
Console(config-if)#end
Console#show ipv6 pim interface
PIM is enabled.
VLAN 1 is up.
PIM Mode                : Dense Mode
IPv6 Address             : None
Hello Interval           : 30 sec
Hello HoldTime           : 105 sec
Triggered Hello Delay    : 5 sec
Join/Prune Holdtime      : 210 sec
Lan Prune Delay          : Disabled
Propagation Delay        : 500 ms
Override Interval        : 2500 ms
Graft Retry Interval     : 3 sec
Max Graft Retries        : 3
State Refresh Ori Int    : 60 sec

Console#

```

ipv6 pim hello-holdtime This command configures the interval to wait for hello messages from a neighboring PIM router before declaring it dead. Use the **no** form to restore the default value.

Syntax

ipv6 pim hello-holdtime *seconds*

no ipv6 pim hello-interval

seconds - The hold time for PIM hello messages. (Range: 1-65535)

Default Setting

105 seconds

Command Mode

Interface Configuration (VLAN)

Command Usage

The **ip pim hello-holdtime** should be greater than the value of **ipv6 pim hello-interval**.

Example

```
Console(config-if)#ipv6 pim hello-holdtime 210
Console(config-if)#
```

ipv6 pim hello-interval This command configures the frequency at which PIM hello messages are transmitted. Use the **no** form to restore the default value.

Syntax

ipv6 pim hello-interval *seconds*

no pimv6 hello-interval

seconds - Interval between sending PIM hello messages. (Range: 1-65535)

Default Setting

30 seconds

Command Mode

Interface Configuration (VLAN)

Command Usage

Hello messages are sent to neighboring PIM routers from which this device has received probes, and are used to verify whether or not these neighbors are still active members of the multicast tree.

Example

```
Console(config-if)#ipv6 pim hello-interval 60
Console(config-if)#
```

ipv6 pim join-prune-holdtime This command configures the hold time for the prune state. Use the **no** form to restore the default value.

Syntax

ipv6 pim join-prune-holdtime *seconds*

no ipv6 pim join-prune-holdtime

seconds - The hold time for the prune state. (Range: 0-65535)

Default Setting

210 seconds

Command Mode

Interface Configuration (VLAN)

Command Usage

The multicast interface that first receives a multicast stream from a particular source forwards this traffic to all other PIM interfaces on the router. If there are no requesting groups on that interface, the leaf node sends a prune message upstream and enters a prune state for this multicast stream. The prune state is maintained until the join-prune-holdtime timer expires or a graft message is received for the forwarding entry.

Example

```
Console(config-if)#ipv6 pim join-prune-holdtime 60
Console(config-if)#
```

**ipv6 pim
lan-prune-delay**

This command causes this device to inform downstream routers of how long it will wait before pruning a flow after receiving a prune request. Use the **no** form to disable this feature.

Syntax**[no] ipv6 pim lan-prune-delay****Default Setting**

Disabled

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ When other downstream routers on the same VLAN are notified that this upstream router has received a prune request, they must send a Join to override the prune before the prune delay expires if they want to continue receiving the flow. The message generated by this command effectively prompts any downstream neighbors with hosts receiving the flow to reply with a Join message. If no join messages are received after the prune delay expires, this router will prune the flow.
- ◆ Prune delay is the sum of the effective propagation-delay and effective override-interval, where effective propagation-delay is the largest propagation-delay from those advertised by each neighbor (including this switch), and effective override-interval is the largest override-interval from those advertised by each neighbor (including this switch).

Example

```
Console(config-if)#ipv6 pim lan-prune-delay  
Console(config-if)#
```

Related Commands

[ipv6 pim override-interval \(1048\)](#)

[ipv6 pim propagation-delay \(1049\)](#)

ipv6 pim override-interval This command configures the override interval, or the time it takes a downstream router to respond to a lan-prune-delay message. Use the **no** form to restore the default setting.

Syntax

ipv6 pim override-interval *milliseconds*

no ipv6 pim override-interval

milliseconds - The time required for a downstream router to respond to a lan-prune-delay message by sending back a Join message if it wants to continue receiving the flow referenced in the message. (Range: 500-6000 milliseconds)

Default Setting

2500 milliseconds

Command Mode

Interface Configuration (VLAN)

Command Usage

The override interval configured by this command and the propagation delay configured by the [ipv6 pim propagation-delay](#) command are used to calculate the LAN prune delay. If a downstream router has group members which want to continue receiving the flow referenced in a LAN prune delay message, then the override interval represents the time required for the downstream router to process the message and then respond by sending a Join message back to the upstream router to ensure that the flow is not terminated.

Example

```
Console(config-if)#ipv6 pim override-interval 3500  
Console(config-if)#
```

Related Commands

[ipv6 pim propagation-delay \(1049\)](#)

[ipv6 pim lan-prune-delay \(1047\)](#)

ipv6 pim propagation-delay This command configures the propagation delay required for a LAN prune delay message to reach downstream routers. Use the **no** form to restore the default setting.

ipv6 pim propagation-delay *milliseconds*

no ipv6 pim propagation-delay

milliseconds - The time required for a lan-prune-delay message to reach downstream routers attached to the same VLAN interface. (Range: 100-5000 milliseconds)

Default Setting

500 milliseconds

Command Mode

Interface Configuration (VLAN)

Command Usage

The override interval configured by the [ipv6 pim override-interval](#) command and the propagation delay configured by this command are used to calculate the LAN prune delay. If a downstream router has group members which want to continue receiving the flow referenced in a LAN prune delay message, then the propagation delay represents the time required for the lan-prune-delay message to be propagated down from the upstream router to all downstream routers attached to the same VLAN interface.

Example

```
Console(config-if)#ipv6 pim propagation-delay 600
Console(config-if)#
```

Related Commands

[ipv6 pim override-interval \(1048\)](#)

[ipv6 pim lan-prune-delay \(1047\)](#)

ipv6 pim trigger-hello-delay This command configures the maximum time before transmitting a triggered PIM Hello message after the router is rebooted or PIM is enabled on an interface. Use the **no** form to restore the default value.

Syntax

ipv6 pim trigger-hello-delay *seconds*

no ipv6 pim trigger-hello-delay

seconds - The maximum time before sending a triggered PIM Hello message. (Range: 0-5)

Default Setting

5 seconds

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ When a router first starts or PIM is enabled on an interface, the hello delay is set to random value between 0 and the trigger-hello-delay. This prevents synchronization of Hello messages on multi-access links if multiple routers are powered on simultaneously.
- ◆ Also, if a Hello message is received from a new neighbor, the receiving router will send its own Hello message after a random delay between 0 and the trigger-hello-delay.

Example

```
Console(config-if)#ipv6 pim trigger-hello-delay 3
Console(config-if)#
```

show ipv6 pim interface This command displays information about interfaces configured for PIM.

Syntax

show ipv6 pim [interface vlan *vlan-id*]

vlan-id - VLAN ID (Range: 1-4094)

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command displays the PIM settings for the specified interface as described in the preceding pages. It also shows the address of the designated PIM router and the number of neighboring PIM routers.

Example

```
Console#show ipv6 pim interface vlan 1
PIM is enabled.
VLAN 1 is up.
PIM Mode                : Dense Mode
IPv6 Address             : fe80::7272:cfff:fe8c:2fef%1
Hello Interval           : 30 sec
Hello HoldTime           : 105 sec
Triggered Hello Delay    : 5 sec
Join/Prune Holdtime      : 210 sec
Lan Prune Delay          : Disabled
Propagation Delay        : 500 ms
Override Interval        : 2500 ms
Graft Retry Interval     : 3 sec
Max Graft Retries        : 3
State Refresh Ori Int    : 60 sec

Console#
```

show ipv6 pim neighbor This command displays information about PIM neighbors.

Syntax

show ipv6 pim neighbor [**interface vlan** *vlan-id*]

vlan-id - VLAN ID (Range: 1-4094)

Default Setting

Displays information for all known PIM neighbors.

Command Mode

Normal Exec, Privileged Exec

Example

```

Console#show ipv6 pim neighbor
Neighbor Address          VLAN Interface Uptime   Expire   DR
-----
FF80::0101                VLAN 1        00:01:23 00:01:23 YES
FF80::0202                VLAN 2        1d 11h   Never
Console#

```

Table 215: show ipv6 pim neighbor - display description

Field	Description
Neighbor Address	IP address of the next-hop router.
VLAN Interface	Interface number that is attached to this neighbor.
Uptime	The duration this entry has been active.
Expiration Time	The time before this entry will be removed.
DR	The designated PIM6-SM router. If multicast hosts are directly connected to the LAN, then only one of these routers is elected as the DR, and acts on behalf of these hosts, sending periodic Join/Prune messages toward a group-specific RP for each group.

PIM6-DM Commands

ipv6 pim graft-retry-interval This command configures the time to wait for a Graft acknowledgement before resending a Graft. Use the **no** form to restore the default value.

Syntax

ipv6 pim graft-retry-interval *seconds*

no ipv6 pim graft-retry-interval

seconds - The time before resending a Graft. (Range: 1-10 seconds)

Default Setting

3 seconds

Command Mode

Interface Configuration (VLAN)

Command Usage

A graft message is sent by a router to cancel a prune state. When a router receives a graft message, it must respond with an graft acknowledgement message. If this acknowledgement message is lost, the router that sent the graft message will resend it a number of times (as defined by the [ipv6 pim max-graft-retries](#) command).

Example

```
Console(config-if)#ipv6 pim graft-retry-interval 9
Console(config-if)#
```

Related Commands

[ipv6 pim override-interval \(1048\)](#)

[ipv6 pim propagation-delay \(1049\)](#)

ipv6 pim max-graft-retries

This command configures the maximum number of times to resend a Graft message if it has not been acknowledged. Use the **no** form to restore the default value.

Syntax

ipv6 pim max-graft-retries *retries*

no ipv6 pim max-graft-retries

retries - The maximum number of times to resend a Graft. (Range: 1-10)

Default Setting

3

Command Mode

Interface Configuration (VLAN)

Example

```
Console(config-if)#ipv6 pim max-graft-retries 5
Console(config-if)#
```

ipv6 pim state-refresh origination-interval This command sets the interval between sending PIM-DM state refresh control messages. Use the **no** form to restore the default value.

Syntax

ipv6 pim state-refresh origination-interval *seconds*

no ipv6 pim max-graft-retries

seconds - The interval between sending PIM-DM state refresh control messages. (Range: 1-100 seconds)

Default Setting

60 seconds

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ The pruned state times out approximately every three minutes and the entire PIM-DM network is reflooded with multicast packets and prune messages. The state refresh feature keeps the pruned state from timing out by periodically forwarding a control message down the distribution tree, refreshing the prune state on the outgoing interfaces of each router in the tree. This also enables PIM routers to recognize topology changes (sources joining or leaving a multicast group) before the default three-minute state timeout expires.
- ◆ This command is only effectively for interfaces of first hop, PIM-DM routers that are directly connected to sources of multicast groups.

Example

```
Console(config-if)#ipv6 pim state-refresh origination-interval 30
Console(config-if)#
```

PIM6-SM Commands

ipv6 pim bsr-candidate This command configures the switch as a Bootstrap Router (BSR) candidate. Use the **no** form to restore the default value.

Syntax

**ipv6 pim bsr-candidate interface vlan *vlan-id* [*hash hash-mask-length*]
[*priority priority*]**

no ipv6 pim bsr-candidate

vlan-id - VLAN ID (Range: 1-4094)

hash-mask-length - Hash mask length (in bits) used for RP selection (see [ipv6 pim rp-candidate](#) and [ipv6 pim rp-address](#)). The portion of the hash specified by the mask length is ANDed with the group address. Therefore, when the hash function is executed on any BSR, all groups with the same seed hash will be mapped to the same RP. If the mask length is less than 32, then only the first portion of the hash is used, and a single RP will be defined for multiple groups. (Range: 0-32 bits)

priority - Priority used by the candidate bootstrap router in the election process. The BSR candidate with the largest priority is preferred. If the priority values are the same, the candidate with the larger IP address is elected to be the BSR. Setting the priority to zero means that this router is not eligible to server as the BSR. At least one router in the PIM6-SM domain must be set to a value greater than zero. (Range: 0-255)

Default Setting

Hash Mask Length: 10

Priority: 0

Command Mode

Global Configuration

Command Usage

- ◆ When the **ipv6 pim bsr-candidate** command is entered, the router starts sending bootstrap messages to all of its PIM6-SM neighbors. The IP address of the designated VLAN is sent as the candidate's BSR address. Each neighbor receiving the bootstrap message compares the BSR address with the address from previous messages. If the current address is the same or a higher address, it accepts the bootstrap message and forwards it. Otherwise, it drops the message.
- ◆ This router will continue to be the BSR until it receives a bootstrap message from another candidate with a higher priority (or a higher IP address if the priorities are the same).
- ◆ To improve failover recovery, it is advisable to select at least two core routers in diverse locations, each to serve as both a candidate BSR and candidate RP. It is also preferable to set up one of these routers as both the primary BSR and RP.

Example

The following example configures the router to start sending bootstrap messages out of the interface for VLAN 1 to all of its PIM-SM neighbors.

```
Console(config)#ipv6 pim bsr-candidate interface vlan 1 hash 20 priority 200
Console(config)#exit
Console#show ipv6 pim bsr-router
PIMv2 Bootstrap information
BSR Address       : 2001:DB8:2222:7272::72
Uptime           : 00:00:08
BSR Priority      : 200
Hash Mask Length : 20
Expire           : 00:00:57
Role             : Candidate BSR
State            : Elected BSR
Console#
```

ipv6 pim register-rate-limit

This command configures the rate at which register messages are sent by the Designated Router (DR) for each (source, group) entry. Use the **no** form to restore the default value.

Syntax

ipv6 pim register-rate-limit *rate*

no ipv6 pim register-rate-limit

rate - The maximum number of register packets per second.
(Range: 1-65535; Default: 0, which means no limit)

Default Setting

0

Command Mode

Global Configuration

Command Usage

This command can be used to relieve the load on the Designated Router (DR) and RP. However, because register messages exceeding the limit are dropped, some receivers may experience data packet loss within the first few seconds in which register messages are sent from bursty sources.

Example

This example sets the register rate limit to 500 pps.

```
Console(config)#ipv6 pim register-rate-limit 500
Console(config)#
```

ipv6 pim register-source This command configures the IP source address of a register message to an address other than the outgoing interface address of the designated router (DR) that leads back toward the rendezvous point (RP). Use the **no** form to restore the default setting.

Syntax

ipv6 pim register-source interface vlan *vlan-id*

no ipv6 pim register-source

vlan-id - VLAN ID (Range: 1-4094)

Default Setting

The IP address of the DR's outgoing interface that leads back to the RP

Command Mode

Global Configuration

Command Usage

When the source address of a register message is filtered by intermediate network devices, or is not a uniquely routed address to which the RP can send packets, the replies sent from the RP to the source address will fail to reach the DR, resulting in PIM6-SM protocol failures. This command can be used to overcome this type of problem by manually configuring the source address of register messages to an interface that leads back to the RP.

Example

This example sets the register source address to the interface address for VLAN 1.

```
Console(config)#ipv6 pim register-source interface vlan 1
Console(config)#
```

ipv6 pim rp-address This command sets a static address for the Rendezvous Point (RP) for a particular multicast group. Use the **no** form to remove an RP address or an RP address for a specific group.

Syntax

[no] ipv6 pim rp-address *rp-address* [group-prefix *group-prefix*]

rp-address - Static IPv6 address of the router that will be an RP for the specified multicast group(s).

group-prefix - An IPv6 network prefix for a multicast group. If a group prefix is not specified, the RP is used for all multicast groups.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ The router specified by this command will act as an RP for all multicast groups in the local PIM6-SM domain if no groups are specified. A static RP can either be configured for the whole multicast group range FF00::/8, or for specific group ranges.
- ◆ Using this command to configure multiple static RPs with the same RP address is not allowed. If an IP address is specified that was previously used for an RP, then the older entry is replaced. (
- ◆ Multiple RPs can be defined for different groups or group ranges. If a group is matched by more than one entry, the router will use the RP associated with the longer group prefix length. If the prefix lengths are the same, then the static RP with the highest IP address is chosen.
- ◆ Static definitions for RP addresses may be used together with RP addresses dynamically learned through the bootstrap router (BSR). If an RP address learned by the BSR and one statically configured using this command are both available for a group range, the RP address learned by the BSR is chosen over the one statically configured with this command.
- ◆ All routers within the same PIM6-SM domain must be configured with the same RP(s). Selecting an RP through the dynamic election process is therefore preferable for most situations. Using the dynamic RP election process also allows a backup RP to automatically take over if the active RP router becomes unavailable.
- ◆ If the **no** form of this command is used without specifying a multicast group, all multicast groups are removed.

Example

In the following example, the first PIM-SM command just specifies the RP address 192.168.1.1 to indicate that it will be used to service all multicast groups. The second PIM-SM command includes the multicast groups to be serviced by the RP.

```
Console(config)#ipv6 pim rp-address 2001:DB8:2222:7272::72
Console(config)#ipv6 pim rp-address 2001:DB8:2222:7272::72 group-prefix
  FFAA::0101/8
Console(config)#end
Console#show ipv6 pim rp mapping
PIM Group-to-RP Mappings
Groups          : FF00::/8
RP address      : 2001:DB8:2222:7272::72/128
Info source     : static
Uptime         : 00:03:10
Expire         : Never
Console#
```

ipv6 pim rp-candidate This command configures the router to advertise itself as a Rendezvous Point (RP) candidate to the bootstrap router (BSR). Use the **no** form to remove this router as an RP candidate.

Syntax

ipv6 pim rp-candidate interface vlan *vlan-id*
[**group-prefix** *group-prefix*] [**interval** *seconds*] [**priority** *value*]

no ipv6 pim rp-candidate interface vlan *vlan-id*

vlan-id - VLAN ID (Range: 1-4094)

group-prefix - An IPv6 network prefix for a multicast group. If a group prefix is not specified, the RP is advertised for all multicast groups.

seconds - The interval at which this device advertises itself as an RP candidate. (Range: 60-16383 seconds)

value - Priority used by the candidate RP in the election process. The RP candidate with the largest priority is preferred. If the priority values are the same, the candidate with the larger IP address is elected to be the RP. Setting the priority to zero means that this router is not eligible to server as the RP. (Range: 0-255)

Default Setting

Interval: 60 seconds

Priority: 0

Command Mode

Global Configuration

Command Usage

- ◆ When the **ipv6 pim rp-candidate** command is entered, the router periodically sends PIMv2 messages to the BSR advertising itself as a candidate RP for the specified group addresses. The IP address of the designated VLAN is sent as the candidate's RP address. The BSR places information about all of the candidate RPs in subsequent bootstrap messages. The BSR uses the RP-election hash algorithm to select an active RP for each group range. The election process is performed by the BSR only for its own use. Each PIM-SM router that receives the list of RP candidates from the BSR also elects an active RP for each group range using the same election process.
- ◆ The election process for each group is based on the following criteria:
 - Find all RPs with the most specific group range.
 - Select those with the highest priority (lowest priority value).
 - Compute a hash value based on the group address, RP address, priority, and hash mask included in the bootstrap messages.
 - If there is a tie, use the candidate RP with the highest IP address.

- ◆ This distributed election process provides faster convergence and minimal disruption when an RP fails. It also serves to provide load balancing by distributing groups across multiple RPs. Moreover, when an RP fails, the responsible RPs are re-elected on each router, and the groups automatically distributed to the remaining RPs.
- ◆ To improve failover recovery, it is advisable to select at least two core routers in diverse locations, each to serve as both a candidate BSR and candidate RP. It is also preferable to set up one of these routers as both the primary BSR and RP.

Example

The following example configures the router to start advertising itself to the BSR as a candidate RP for the indicated multicast groups.

```

Console(config)#ipv6 pim rp-candidate interface vlan 1 group-prefix
FFAA::0101/8
Console(config)#end
Console#show ipv6 pim rp mapping
PIM Group-to-RP Mappings
Groups          : FF00::/8
RP address      : 2001:DB8:2222:7272::72/128
Info source     : 2001:DB8:2222:7272::72/128, via bootstrap, priority: 0
Uptime         : 00:02:35
Expire          : 00:01:55
Console#

```

ipv6 pim spt-threshold

This command prevents the last-hop PIM router from switching to Shortest Path Source Tree (SPT) mode. Use the **no** form to allow the router to switch over to SPT mode.

Syntax

ipv6 pim spt-threshold infinity [**group-prefix** *group-prefix*]

no ipv6 pim spt-threshold infinity

group-prefix - An IPv6 network prefix for a multicast group. If a group address is not specified, the command applies to all multicast groups.

Default Setting

The last-hop PIM6 router joins the shortest path tree immediately after the first packet arrives from a new source.

Command Mode

Global Configuration

Command Usage

- ◆ The default path for packets from a multicast source to a receiver is through the RP. However, the path through the RP is not always the shortest path. Therefore, the router uses the RP to forward only the first packet from a new multicast group to its receivers. Afterwards, it calculates the shortest path tree (SPT)

directly between the receiver and source, and then uses the SPT to send all subsequent packets from the source to the receiver instead of using the shared tree. Note that when the SPT threshold is not set by this command, the PIM leaf router will join the shortest path tree immediately after receiving the first packet from a new source.

- ◆ This command forces the router to use the shared tree for all multicast groups, or just for the specified multicast groups.
- ◆ Only one entry is allowed for this command.

Example

This example prevents the switch from using the SPT for multicast groups 2001:DB8:3333:7373::73/96.

```
Console(config)#ipv6 pim spt-threshold infinity group-prefix  
2001:DB8:3333:7373::73/96  
Console#
```

ipv6 pim dr-priority This command sets the priority value for a Designated Router (DR) candidate. Use the **no** form to restore the default setting.

Syntax

ipv6 pim dr-priority *priority-value*

no ipv6 pim dr-priority

priority-value - Priority advertised by a router when bidding to become the DR. (Range: 0-4294967294)

Default Setting

1

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ More than one PIM-SM router may be connected to an Ethernet or other shared-media LAN. If multicast hosts are directly connected to the LAN, then only one of these routers is elected as the DR, and acts on behalf of these hosts, sending periodic Join/Prune messages toward a group-specific RP for each group. A single DR is elected per interface (LAN or otherwise) using a simple election process.
- ◆ The router with the highest priority configured on an interface is elected as the DR. If more than one router attached to this interface uses the same priority, then the router with the highest IP address is elected to serve as the DR.

- ◆ If a router does not advertise a priority in its hello messages, it is assumed to have the highest priority and is elected as the DR. If more than one router is not advertising its priority, then the router with the highest IP address is elected to serve as the DR.

Example

This example sets the priority used in the bidding process for the DR.

```

Console(config)#interface vlan 1
Console(config-if)#ipv6 pim dr-priority 20
Console(config-if)#end
Console#show ipv6 pim interface
PIM is enabled.
VLAN 1 is up.
PIM Mode                : Sparse Mode
IPv6 Address             : FE80::200:E8FF:FE93:82A0
Hello Interval           : 30 sec
Hello HoldTime           : 105 sec
Triggered Hello Delay    : 5 sec
Join/Prune Holdtime      : 210 sec
Lan Prune Delay          : Disabled
Propagation Delay        : 500 ms
Override Interval        : 2500 ms
DR Priority               : 20
Join/Prune Interval      : 60 sec

Console#

```

ipv6 pim join-prune-interval This command sets the join/prune timer. Use the **no** form to restore the default setting.

Syntax

ipv6 pim join-prune-interval *seconds*

no ipv6 pim join-prune-interval

seconds - The interval at which join/prune messages are sent.
(Range: 1-65535 seconds)

Default Setting

60 seconds

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ By default, the switch sends join/prune messages every 210 seconds to inform other PIM-SM routers about clients who want to join or leave a multicast group.
- ◆ Use the same join/prune message interval on all the PIM-SM routers in the same PIM-SM domain, otherwise the routing protocol's performance will be adversely affected.

- ◆ The multicast interface that first receives a multicast stream from a particular source forwards this traffic only to those interfaces on the router that have requested to join this group. When there are no longer any requesting groups on that interface, the leaf node sends a prune message upstream and enters a prune state for this multicast stream. The protocol maintains both the current join state and the pending Reverse Path Tree (RPT) prune state for this (source, group) pair until the join/prune-interval timer expires.

Example

This example sets the priority used in the bidding process for the DR.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 pim join-prune-interval 220
Console#show ipv6 pim interface
PIM is enabled.
VLAN 1 is up.
PIM Mode                : Sparse Mode
IPv6 Address             : FE80::200:E8FF:FE93:82A0
Hello Interval           : 30 sec
Hello HoldTime           : 105 sec
Triggered Hello Delay    : 5 sec
Join/Prune Holdtime      : 210 sec
Lan Prune Delay          : Disabled
Propagation Delay        : 500 ms
Override Interval        : 2500 ms
DR Priority               : 1
Join/Prune Interval      : 220 sec

Console#
```

clear ipv6 pim bsr rp-set This command clears multicast group to RP mapping entries learned through the PIMv2 bootstrap router (BSR).

Command Mode

Privileged Exec

Command Usage

- ◆ This command can be used to update entries in the static multicast forwarding table immediately after making configuration changes to the RP.
- ◆ Use the [show ipv6 pim rp mapping](#) command to display active RPs that are cached with associated multicast routing entries.

Example

This example clears the RP map.

```
Console#clear ipv6 pim bsr rp-set
Console#show ipv6 pim rp mapping
PIM Group-to-RP Mappings
Console#
```

show ipv6 pim bsr-router This command displays information about the bootstrap router (BSR).

Command Mode
Privileged Exec

Command Usage
This command displays information about the elected BSR.

Example
This example displays information about the BSR.

```

Console#show ipv6 pim bsr-router
PIMv2 Bootstrap information
BSR address      : 2001:DB8:2222:7272::72/128
Uptime          : 00:00:04
BSR Priority     : 200
Hash mask length : 20
Expire          : 00:02:06
Role            : Candidate BSR
State           : Elected BSR
Console#

```

Table 216: show ip pim bsr-router - display description

Field	Description
BSR Address	IP address of interface configured as the BSR.
Uptime	The time this BSR has been up and running.
BSR Priority	Priority assigned to this interface for use in the BSR election process.
Hash Mask Length	The number of significant bits used in the multicast group comparison mask. This mask determines the multicast group for which this router can be a BSR.
Expire	The time before this entry will be removed.
Role	Candidate BSR or Non-candidate BSR.
State	Operation state of BSR includes: <ul style="list-style-type: none"> ◆ No information – No information stored for this device. ◆ Accept Any – The router does not know of an active BSR, and will accept the first bootstrap message it sees as giving the new BSR's identity and the RP-set. ◆ Accept Preferred – The router knows the identity of the current BSR, and is using the RP-set provided by that BSR. Only bootstrap messages from that BSR or from a C-BSR with higher weight than the current BSR will be accepted. ◆ Candidate BSR – Bidding in election process. ◆ Pending-BSR – The router is a candidate to be the BSR for the RP-set. Currently, no other router is the preferred BSR, but this router is not yet the elected BSR. ◆ Elected BSR – elected to serve as BSR

show ipv6 pim rp mapping This command displays active RPs and associated multicast routing entries.

Command Mode
Privileged Exec

Example
This example displays the RP map.

```
Console#show ipv6 pim rp mapping
PIM Group-to-RP Mappings
Groups          : FF00::/8
RP address      : 2001:DB8:2222:7272::72/128
Info source     : static
Uptime         : 00:23:21
Expire         : Never
Console#
```

Table 217: show ip pim rp mapping - display description

Field	Description
Groups	The multicast group address, mask length managed by the RP.
RP address	IP address of the RP used for the listed multicast group
Info source	RP that advertised the mapping, how the RP was selected (Static or Bootstrap), and the priority used in the bidding process
Uptime	The time this RP has been up and running
Expire	The time before this entry will be removed

show ipv6 pim rp-hash This command displays the RP used for the specified multicast group, and the RP that advertised the mapping.

Syntax

show ipv6 pim rp-hash *group-address*
group-address - An IP multicast group address.

Command Mode
Privileged Exec

Example
This example displays the RP used for the specified group.

```
Console#show ipv6 pim rp-hash FF00::
RP address      : 2001:DB8:2222:7272::72/128
Info source     : 2001:1::0101, via bootstrap
Console#
```


Table 218: show ip pim rp-hash - display description

Field	Description
RP address	IP address of the RP used for the specified multicast group
Info source	RP that advertised the mapping, and how the RP was selected

Section III

Appendices

This section provides additional information and includes these items:

- ◆ [“Troubleshooting” on page 1069](#)
- ◆ [“License Information” on page 1071](#)



Troubleshooting

Problems Accessing the Management Interface

Table 219: Troubleshooting Chart

Symptom	Action
Cannot connect using Telnet, or SNMP software	<ul style="list-style-type: none">◆ Be sure the switch is powered up.◆ Check network cabling between the management station and the switch. Make sure the ends are properly connected and there is no damage to the cable. Test the cable if necessary.◆ Check that you have a valid network connection to the switch and that the port you are using has not been disabled.◆ Be sure you have configured the VLAN interface through which the management station is connected with a valid IP address, subnet mask and default gateway.◆ Be sure the management station has an IP address in the same subnet as the switch's IP interface to which it is connected.◆ If you are trying to connect to the switch via the IP address for a tagged VLAN group, your management station, and the ports connecting intermediate switches in the network, must be configured with the appropriate tag.◆ If you cannot connect using Telnet, you may have exceeded the maximum number of concurrent Telnet/SSH sessions permitted. Try connecting again at a later time.
Cannot connect using Secure Shell	<ul style="list-style-type: none">◆ If you cannot connect using SSH, you may have exceeded the maximum number of concurrent Telnet/SSH sessions permitted. Try connecting again at a later time.◆ Be sure the control parameters for the SSH server are properly configured on the switch, and that the SSH client software is properly configured on the management station.◆ Be sure you have generated both an RSA and DSA public key on the switch, exported this key to the SSH client, and enabled SSH service. Try using another SSH client or check for updates to your SSH client application.◆ Be sure you have set up an account on the switch for each SSH user, including user name, authentication level, and password.◆ Be sure you have imported the client's public key to the switch (if public key authentication is used).
Cannot access the on-board configuration program via a serial port connection	<ul style="list-style-type: none">◆ Be sure you have set the terminal emulator program to VT100 compatible, 8 data bits, 1 stop bit, no parity, and the baud rate set to 115200 bps.◆ Verify that you are using the RJ-45 to DB-9 null-modem serial cable supplied with the switch. If you use any other cable, be sure that it conforms to the pin-out connections provided in the Installation Guide.
Forgot or lost the password	<ul style="list-style-type: none">◆ Contact your local distributor.

Using System Logs

If a fault does occur, refer to the Installation Guide to ensure that the problem you encountered is actually caused by the switch. If the problem appears to be caused by the switch, follow these steps:

1. Enable logging.
2. Set the error messages reported to include all categories.
3. Enable SNMP.
4. Enable SNMP traps.
5. Designate the SNMP host that is to receive the error messages.
6. Repeat the sequence of commands or other actions that lead up to the error.
7. Make a list of the commands or circumstances that led to the fault. Also make a list of any error messages displayed.
8. Set up your terminal emulation software so that it can capture all console output to a file. Then enter the “show tech-support” command to record all system settings in this file.
9. Contact your distributor’s service engineer, and send a detailed description of the problem, along with the file used to record your system settings.

For example:

```
Console(config)#logging on
Console(config)#logging history flash 7
Console(config)#snmp-server host 192.168.1.23
:
```



License Information

This product includes copyrighted third-party software subject to the terms of the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other related free software licenses. The GPL code used in this product is distributed WITHOUT ANY WARRANTY and is subject to the copyrights of one or more authors. For details, refer to the section "The GNU General Public License" below, or refer to the applicable license as included in the source-code archive.

The GNU General Public License

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

1. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

2. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

3. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
 - a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
 - b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
 - c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

4. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
 - a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

- 5. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
- 6. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.
- 7. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
- 8. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

9. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
10. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.
11. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

1. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
2. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Glossary

ACL Access Control List. ACLs can limit network traffic and restrict access to certain users or devices by checking each packet for certain IP or MAC (i.e., Layer 2) information.

ARP Address Resolution Protocol converts between IP addresses and MAC (hardware) addresses. ARP is used to locate the MAC address corresponding to a given IP address. This allows the switch to use IP addresses for routing decisions and the corresponding MAC addresses to forward packets from one hop to the next.

BOOTP Boot Protocol. BOOTP is used to provide bootup information for network devices, including IP address information, the address of the TFTP server that contains the devices system files, and the name of the boot file.

CoS Class of Service is supported by prioritizing packets based on the required level of service, and then placing them in the appropriate output queue. Data is transmitted from the queues using weighted round-robin service to enforce priority service and prevent blockage of lower-level queues. Priority may be set according to the port default, the packet's priority bit (in the VLAN tag), TCP/UDP port number, IP Precedence bit, or DSCP priority bit.

DHCP Dynamic Host Control Protocol. Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

DHCP Option 82 A relay option for sending information about the requesting client (or an intermediate relay agent) in the DHCP request packets forwarded by the switch and in reply packets sent back from the DHCP server. This information can be used by DHCP servers to assign fixed IP addresses, or set other services or policies for clients.

DHCP Snooping A technique used to enhance network security by snooping on DHCP server messages to track the physical location of hosts, ensure that hosts only use the IP addresses assigned to them, and ensure that only authorized DHCP servers are accessible.

- DiffServ** Differentiated Services provides quality of service on large networks by employing a well-defined set of building blocks from which a variety of aggregate forwarding behaviors may be built. Each packet carries information (DS byte) used by each hop to give it a particular forwarding treatment, or per-hop behavior, at each network node. DiffServ allocates different levels of service to users on the network with mechanisms such as traffic meters, shapers/droppers, packet markers at the boundaries of the network.
- DNS** Domain Name Service. A system used for translating host names for network nodes into IP addresses.
- DSCP** Differentiated Services Code Point Service. DSCP uses a six-bit tag to provide for up to 64 different forwarding behaviors. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP bits are mapped to the Class of Service categories, and then into the output queues.
- EAPOL** Extensible Authentication Protocol over LAN. EAPOL is a client authentication protocol used by this switch to verify the network access rights for any device that is plugged into the switch. A user name and password is requested by the switch, and then passed to an authentication server (e.g., RADIUS) for verification. EAPOL is implemented as part of the IEEE 802.1X Port Authentication standard.
- EUI** Extended Universal Identifier is an address format used by IPv6 to identify the host portion of the network address. The interface identifier in EUI compatible addresses is based on the link-layer (MAC) address of an interface. Interface identifiers used in global unicast and other IPv6 address types are 64 bits long and may be constructed in the EUI-64 format. The modified EUI-64 format interface ID is derived from a 48-bit link-layer address by inserting the hexadecimal number FFFE between the upper three bytes (OUI field) and the lower 3 bytes (serial number) of the link layer address. To ensure that the chosen address is from a unique Ethernet MAC address, the 7th bit in the high-order byte is set to 1 (equivalent to the IEEE Global/Local bit) to indicate the uniqueness of the 48-bit address.
- GARP** Generic Attribute Registration Protocol. GARP is a protocol that can be used by endstations and switches to register and propagate multicast group membership information in a switched environment so that multicast data frames are propagated only to those parts of a switched LAN containing registered endstations. Formerly called Group Address Registration Protocol.
- GMRP** Generic Multicast Registration Protocol. GMRP allows network devices to register end stations with multicast groups. GMRP requires that any participating network devices or end stations comply with the IEEE 802.1p standard.
- GVRP** GARP VLAN Registration Protocol. Defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports along the Spanning Tree so that VLANs defined in each switch can work automatically over a Spanning Tree network.

- ICMP** Internet Control Message Protocol is a network layer protocol that reports errors in processing IP packets. ICMP is also used by routers to feed back information about better routing choices.
- IEEE 802.1D** Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.
- IEEE 802.1Q** VLAN Tagging—Defines Ethernet frame tags which carry VLAN information. It allows switches to assign endstations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.
- IEEE 802.1p** An IEEE standard for providing quality of service (QoS) in Ethernet networks. The standard uses packet tags that define up to eight traffic classes and allows switches to transmit packets based on the tagged priority value.
- IEEE 802.1s** An IEEE standard for the Multiple Spanning Tree Protocol (MSTP) which provides independent spanning trees for VLAN groups.
- IEEE 802.1w** An IEEE standard for the Rapid Spanning Tree Protocol (RSTP) which reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard. (Now incorporated in IEEE 802.1D-2004)
- IEEE 802.1X** Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.
- IEEE 802.3ac** Defines frame extensions for VLAN tagging.
- IEEE 802.3x** Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links. (Now incorporated in IEEE 802.3-2002)
- IGMP** Internet Group Management Protocol. A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast switch/router on a given subnetwork, one of the devices is made the “querier” and assumes responsibility for keeping track of group membership.
- IGMP Proxy** Proxies multicast group membership information onto the upstream interface based on IGMP messages monitored on downstream interfaces, and forwards multicast traffic based on that information. There is no need for multicast routing protocols in a simple tree that uses IGMP Proxy.

IGMP Query On each subnetwork, one IGMP-capable device will act as the querier — that is, the device that asks all hosts to report on the IP multicast groups they wish to join or to which they already belong. The elected querier will be the device with the lowest IP address in the subnetwork.

IGMP Snooping Listening to IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to identify IP Multicast group members.

In-Band Management Management of the network from a station attached directly to the network.

IP Multicast Filtering A process whereby this switch can pass multicast traffic along to participating hosts.

IP Precedence The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The eight values are mapped one-to-one to the Class of Service categories by default, but may be configured differently to suit the requirements for specific network applications.

LACP Link Aggregation Control Protocol. Allows ports to automatically negotiate a trunked link with LACP-configured ports on another device.

Layer 2 Data Link layer in the ISO 7-Layer Data Communications Protocol. This is related directly to the hardware interface for network devices and passes on traffic based on MAC addresses.

Layer 3 Network layer in the ISO 7-Layer Data Communications Protocol. This layer handles the routing functions for data moving from one open system to another.

Link Aggregation *See Port Trunk.*

LLDP Link Layer Discovery Protocol is used to discover basic information about neighboring devices in the local broadcast domain by using periodic broadcasts to advertise information such as device identification, capabilities and configuration settings.

MD5 MD5 Message-Digest is an algorithm that is used to create digital signatures. It is intended for use with 32 bit machines and is safer than the MD4 algorithm, which has been broken. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.

MIB Management Information Base. An acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

MRD Multicast Router Discovery is a A protocol used by IGMP snooping and multicast routing devices to discover which interfaces are attached to multicast routers. This process allows IGMP-enabled devices to determine where to send multicast source and group membership messages.

MSTP Multiple Spanning Tree Protocol can provide an independent spanning tree for different VLANs. It simplifies network management, provides for even faster convergence than RSTP by limiting the size of each region, and prevents VLAN members from being segmented from the rest of the group.

Multicast Switching A process whereby the switch filters incoming multicast frames for services for which no attached host has registered, or forwards them to all ports contained within the designated multicast VLAN group.

MVR Multicast VLAN Registration is a method of using a single network-wide multicast VLAN to transmit common services, such as such as television channels or video-on-demand, across a service-provider's network. MVR simplifies the configuration of multicast services by using a common VLAN for distribution, while still preserving security and data isolation for subscribers residing in both the MVR VLAN and other standard or private VLAN groups.

NTP Network Time Protocol provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.

OSPF Open Shortest Path First is a link-state routing protocol that functions better over a larger network such as the Internet, as opposed to distance-vector routing protocols such as RIP. It includes features such as unlimited hop count, authentication of routing updates, and Variable Length Subnet Masks (VLSM).

Out-of-Band Management Management of the network from a station not attached to the network.

Port Authentication *See IEEE 802.1X.*

Port Mirroring A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be studied unobstructively.

Port Trunk Defines a network link aggregation and trunking method which specifies how to create a single high-speed logical link that combines several lower-speed physical links.

Private VLANs Private VLANs provide port-based security and isolation between ports within the assigned VLAN. Data traffic on downlink ports can only be forwarded to, and from, uplink ports.

QinQ QinQ tunneling is designed for service providers carrying traffic for multiple customers across their networks. It is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs.

QoS Quality of Service. QoS refers to the capability of a network to provide better service to selected traffic flows using features such as data prioritization, queuing, congestion avoidance and traffic shaping. These features effectively provide preferential treatment to specific flows either by raising the priority of one flow or limiting the priority of another flow.

RADIUS Remote Authentication Dial-in User Service. RADIUS is a logon authentication protocol that uses software running on a central server to control access to RADIUS-compliant devices on the network.

RIP Routing Information Protocol seeks to find the shortest route to another device by minimizing the distance-vector, or hop count, which serves as a rough estimate of transmission cost. RIP-2 is a compatible upgrade to RIP. It adds useful capabilities for subnet routing, authentication, and multicast transmissions.

RMON Remote Monitoring. RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP, and can set alarms on a variety of traffic conditions, including specific error types.

RSTP Rapid Spanning Tree Protocol. RSTP reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard.

SMTP Simple Mail Transfer Protocol is a standard host-to-host mail transport protocol that operates over TCP, port 25.

SNMP Simple Network Management Protocol. The application protocol in the Internet suite of protocols which offers network management services.

- SNTP** Simple Network Time Protocol allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.
- SSH** Secure Shell is a secure replacement for remote access functions, including Telnet. SSH can authenticate users with a cryptographic key, and encrypt data connections between management clients and the switch.
- STA** Spanning Tree Algorithm is a technology that checks your network for any loops. A loop can often occur in complicated or backup linked network systems. Spanning Tree detects and directs data along the shortest available path, maximizing the performance and efficiency of the network.
- TACACS+** Terminal Access Controller Access Control System Plus. TACACS+ is a logon authentication protocol that uses software running on a central server to control access to TACACS-compliant devices on the network.
- TCP/IP** Transmission Control Protocol/Internet Protocol. Protocol suite that includes TCP as the primary transport protocol, and IP as the network layer protocol.
- Telnet** Defines a remote communication facility for interfacing to a terminal device over TCP/IP.
- TFTP** Trivial File Transfer Protocol. A TCP/IP protocol commonly used for software downloads.
- UDP** User Datagram Protocol. UDP provides a datagram mode for packet-switched communications. It uses IP as the underlying transport mechanism to provide access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.
- UTC** Universal Time Coordinate. UTC is a time scale that couples Greenwich Mean Time (based solely on the Earth's rotation rate) with highly accurate atomic time. The UTC does not have daylight saving time.
- VLAN** Virtual LAN. A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, and allows users to share information and resources as though located on the same LAN.

VRRP Virtual Router Redundancy Protocol uses a virtual IP address to support a primary router and multiple backup routers. The backups can be configured to take over the workload if the master fails or to load share the traffic. The primary goal of VRRP is to allow a host device which has been configured with a fixed gateway to maintain network connectivity in case the primary gateway goes down.

XModem A protocol used to transfer files between devices. Data is grouped in 128-byte blocks and error-corrected.

Index of CLI Commands

A

aaa accounting dot1x 230
aaa accounting exec 231
aaa accounting update 232
aaa authorization exec 233
aaa group server 234
abr-type 883
absolute 170
access-list arp 364
access-list ip 348
access-list ipv6 354
access-list mac 359
accounting dot1x 235
accounting exec 235
aggregate-address 928
alias 371
area default-cost 845
area default-cost 886
area nssa 851
area range 846
area range 887
area stub 852
area stub 890
area virtual-link 854
area virtual-link 891
arp 757
arp timeout 758
authentication enable 220
authentication login 221
authorization exec 236
auto-cost reference-bandwidth 847
auto-traffic-control 433
auto-traffic-control action 433
auto-traffic-control alarm-clear-threshold 434
auto-traffic-control alarm-fire-threshold 435
auto-traffic-control apply-timer 431
auto-traffic-control auto-control-release 436
auto-traffic-control control-release 437
auto-traffic-control release-timer 432

B

banner configure 103
banner configure company 104
banner configure dc-power-info 105
banner configure department 105
banner configure equipment-info 106
banner configure equipment-location 107
banner configure ip-lan 107
banner configure lp-number 108

banner configure manager-info 109
banner configure mux 109
banner configure note 110
bgp always-compare-med 943
bgp bestpath as-path ignore 944
bgp bestpath compare-confed-aspath 944
bgp bestpath compare-routerid 944
bgp bestpath med 945
bgp client-to-client reflection 930
bgp cluster-id 931
bgp confederation identifier 932
bgp confederation peer 933
bgp dampening 934
bgp default local-preference 946
bgp deterministic-med 946
bgp enforce-first-as 935
bgp fast-external-failover 935
bgp log-neighbor-changes 936
bgp network import-check 936
bgp router-id 937
bgp scan-time 937
boot system 124
bootfile 739
bridge-ext gvrp 478

C

calendar set 167
call 991
capabilities 372
channel-group 404
class 552
class-map 548
clear arp-cache 759
clear counters 385
clear dns cache 726
clear host 726
clear ip bgp 941
clear ip bgp dampening 942
clear ip dhcp binding 747
clear ip dhcp snooping binding 309
clear ip dhcp snooping database flash 309
clear ip igmp group 677
clear ip igmp snooping groups dynamic 608
clear ip igmp snooping statistics 608
clear ip ospf process 845
clear ip pim bsr rp-set 1039
clear ip rip route 836
clear ipv6 dhcp snooping binding 317
clear ipv6 dhcp snooping statistics 317

Index of CLI Commands

clear ipv6 mld group 689
clear ipv6 neighbors 789
clear ipv6 pim bsr rp-set 1062
clear ipv6 traffic 780
clear log 149
clear mac-address-table dynamic 445
clear mvr groups dynamic 645
clear mvr statistics 645
clear mvr6 groups dynamic 664
clear mvr6 statistics 664
clear network-access 292
clear pfc statistics 571
clear pppoe intermediate-agent statistics 271
clear vrrp interface counters 806
clear vrrp router counters 806
client-identifier 739
clock summer-time (date) 163
clock summer-time (predefined) 164
clock summer-time (recurring) 165
clock timezone 167
cluster 173
cluster commander 174
cluster ip-pool 174
cluster member 175
cn 582
cn cnm-transmit-priority 582
cn cnpv 583
cn cnpv alternate-priority (Global Configuration) 584
cn cnpv alternate-priority (Interface Configuration) 586
cn cnpv defense-mode (Global Configuration) 585
cn cnpv defense-mode (Interface Configuration) 587
compatible rfc1583 841
configure 97
continue 992
copy 125

D

databits 135
dcbx 566
dcbx mode 566
default-information originate 822
default-information originate 842
default-metric 823
default-metric 848
default-metric 888
default-router 740
delete 128
delete public-key 248
description 549
description 373
description 992
dir 129
disable 98
disconnect 143
distance 824
distance 947
distance bgp 948

dns-server 741
domain-name 741
dos-protection land 339
dos-protection tcp-null-scan 340
dos-protection tcp-syn-fin-scan 340
dos-protection tcp-xmas-scan 341
dot1q-tunnel system-tunnel-control 494
dot1x default 254
dot1x eapol-pass-through 254
dot1x intrusion-action 255
dot1x max-reauth-req 256
dot1x max-req 256
dot1x operation-mode 257
dot1x port-control 258
dot1x re-authenticate 261
dot1x re-authentication 258
dot1x system-auth-control 255
dot1x timeout quiet-period 259
dot1x timeout re-authperiod 259
dot1x timeout supp-timeout 260
dot1x timeout tx-period 260

E

enable 95
enable password 218
end 99
ets mode 574
exec-timeout 136
exit 99

F

fan-speed force-full 121
flowcontrol 373

G

garp timer 479

H

hardware-address 742
history 374
host 743
hostname 102

I

interface 370
interface tunnel 793
interface vlan 486
ip access-group 352
ip address 750
ip arp inspection 331
ip arp inspection filter 332
ip arp inspection limit 335
ip arp inspection log-buffer logs 333
ip arp inspection trust 336

ip arp inspection validate 334
 ip arp inspection vlan 334
 ip as-path access-list 922
 ip community-list 923
 ip default-gateway 752
 ip dhcp client class-id 729
 ip dhcp excluded-address 737
 ip dhcp pool 738
 ip dhcp relay server 733
 ip dhcp restart client 731
 ip dhcp restart relay 734
 ip dhcp snooping 301
 ip dhcp snooping database flash 310
 ip dhcp snooping information option 303
 ip dhcp snooping information option circuit-id 307
 ip dhcp snooping information policy 304
 ip dhcp snooping trust 308
 ip dhcp snooping verify mac-address 305
 ip dhcp snooping vlan 306
 ip domain-list 721
 ip domain-lookup 722
 ip domain-name 723
 ip extcommunity-list 925
 ip forward-protocol udp 760
 ip helper 761
 ip helper-address 762
 ip host 724
 ip http port 238
 ip http secure-port 239
 ip http secure-server 239
 ip http server 238
 ip igmp 672
 ip igmp filter (Global Configuration) 615
 ip igmp filter (Interface Configuration) 617
 ip igmp last-member-query-interval 673
 ip igmp max-groups 618
 ip igmp max-groups action 619
 ip igmp max-resp-interval 673
 ip igmp profile 616
 ip igmp proxy 681
 ip igmp proxy unsolicited-report-interval 683
 ip igmp query-drop 619
 ip igmp query-interval 674
 ip igmp robustval 675
 ip igmp snooping 593
 ip igmp snooping proxy-reporting 594
 ip igmp snooping querier 594
 ip igmp snooping router-alert-option-check 595
 ip igmp snooping router-port-expire-time 596
 ip igmp snooping tcn-flood 596
 ip igmp snooping tcn-query-solicit 597
 ip igmp snooping unregistered-data-flood 598
 ip igmp snooping unsolicited-report-interval 599
 ip igmp snooping version 599
 ip igmp snooping version-exclusive 600
 ip igmp snooping vlan general-query-suppression 601
 ip igmp snooping vlan immediate-leave 601
 ip igmp snooping vlan last-memb-query-count 602
 ip igmp snooping vlan last-memb-query-intvl 603
 ip igmp snooping vlan mrd 603
 ip igmp snooping vlan mrouter 1017
 ip igmp snooping vlan mrouter 613
 ip igmp snooping vlan proxy-address 604
 ip igmp snooping vlan query-interval 606
 ip igmp snooping vlan query-resp-intvl 606
 ip igmp snooping vlan static 607
 ip igmp static-group 676
 ip igmp version 677
 ip multicast-data-drop 620
 ip multicast-routing 1011
 ip name-server 724
 ip ospf authentication 857
 ip ospf authentication-key 859
 ip ospf cost 860
 ip ospf dead-interval 861
 ip ospf hello-interval 861
 ip ospf message-digest-key 862
 ip ospf priority 863
 ip ospf retransmit-interval 864
 ip ospf transmit-delay 865
 ip pim 1021
 ip pim bsr-candidate 1030
 ip pim dr-priority 1037
 ip pim graft-retry-interval 1028
 ip pim hello-holdtime 1022
 ip pim hello-interval 1023
 ip pim join-prune-holdtime 1023
 ip pim join-prune-interval 1038
 ip pim lan-prune-delay 1024
 ip pim max-graft-retries 1029
 ip pim override-interval 1025
 ip pim propagation-delay 1026
 ip pim register-rate-limit 1032
 ip pim register-source 1032
 ip pim rp-address 1033
 ip pim rp-candidate 1035
 ip pim spt-threshold 1036
 ip pim state-refresh origination-interval 1029
 ip pim trigger-hello-delay 1026
 ip prefix-list 927
 ip proxy-arp 758
 ip rip authentication mode 831
 ip rip authentication string 832
 ip rip receive version 832
 ip rip receive-packet 833
 ip rip send version 834
 ip rip send-packet 835
 ip rip split-horizon 836
 ip route 812
 ip source-guard 321
 ip source-guard binding 320
 ip source-guard max-binding 323
 ip ssh authentication-retries 246
 ip ssh crypto host-key generate 249
 ip ssh crypto zeroize 250
 ip ssh save host-key 250
 ip ssh server 246

Index of CLI Commands

ip ssh server-key size 247
ip ssh timeout 248
ip telnet max-sessions 241
ip telnet port 242
ip telnet server 242
ipv6 access-group 358
ipv6 address 766
ipv6 address eui-64 767
ipv6 address link-local 769
ipv6 default-gateway 765
ipv6 dhcp client rapid-commit vlan 732
ipv6 dhcp relay destination 735
ipv6 dhcp snooping 312
ipv6 dhcp snooping max-binding 315
ipv6 dhcp snooping trust 315
ipv6 dhcp snooping vlan 314
ipv6 enable 770
ipv6 hop-limit 783
ipv6 host 725
ipv6 mld 684
ipv6 mld last-member-query-response-interval 684
ipv6 mld max-resp-interval 685
ipv6 mld proxy 692
ipv6 mld proxy unsolicited-report-interval 694
ipv6 mld query-interval 686
ipv6 mld robustval 687
ipv6 mld snooping 625
ipv6 mld snooping querier 625
ipv6 mld snooping query-interval 626
ipv6 mld snooping query-max-response-time 626
ipv6 mld snooping robustness 627
ipv6 mld snooping router-port-expire-time 627
ipv6 mld snooping unknown-multicast mode 628
ipv6 mld snooping version 629
ipv6 mld snooping vlan immediate-leave 630
ipv6 mld snooping vlan mrouter 629
ipv6 mld snooping vlan static 630
ipv6 mld static-group 687
ipv6 mld version 688
ipv6 mtu 772
ipv6 multicast-routing 1014
ipv6 nd dad attempts 783
ipv6 nd ns-interval 785
ipv6 nd rguard 786
ipv6 nd reachable-time 787
ipv6 neighbor 788
ipv6 ospf cost 895
ipv6 ospf dead-interval 896
ipv6 ospf hello-interval 897
ipv6 ospf priority 897
ipv6 ospf retransmit-interval 898
ipv6 ospf transmit-delay 899
ipv6 pim 1044
ipv6 pim bsr-candidate 1054
ipv6 pim dr-priority 1060
ipv6 pim graft-retry-interval 1051
ipv6 pim hello-holdtime 1045
ipv6 pim hello-interval 1046
ipv6 pim join-prune-holdtime 1046

ipv6 pim join-prune-interval 1061
ipv6 pim lan-prune-delay 1047
ipv6 pim max-graft-retries 1052
ipv6 pim override-interval 1048
ipv6 pim propagation-delay 1049
ipv6 pim register-rate-limit 1055
ipv6 pim register-source 1056
ipv6 pim rp-address 1056
ipv6 pim rp-candidate 1058
ipv6 pim spt-threshold 1059
ipv6 pim state-refresh origination-interval 1053
ipv6 pim trigger-hello-delay 1049
ipv6 route 817
ipv6 router ospf area 893
ipv6 router ospf tag area 894
ipv6 source-guard 326
ipv6 source-guard binding 325
ipv6 source-guard max-binding 328

J

jumbo frame 122

L

l2protocol-tunnel tunnel-dmac 500
lACP 404
lACP admin-key (Ethernet Interface) 406
lACP admin-key (Port Channel) 408
lACP port-priority 406
lACP system-priority 407
lACP timeout 409
lease 744
line 135
lldp 697
lldp admin-status 701
lldp basic-tlv management-ip-address 701
lldp basic-tlv port-description 702
lldp basic-tlv system-capabilities 703
lldp basic-tlv system-description 703
lldp basic-tlv system-name 704
lldp dcBx-tlv ets-config 704
lldp dcBx-tlv ets-recommend 705
lldp dcBx-tlv pfc-config 706
lldp dot1-tlv proto-ident 706
lldp dot1-tlv proto-vid 707
lldp dot1-tlv pvid 707
lldp dot1-tlv vlan-name 708
lldp dot3-tlv link-aggr 708
lldp dot3-tlv mac-phy 709
lldp dot3-tlv max-frame 709
lldp holdtime-multiplier 697
lldp med-fast-start-count 698
lldp med-location civic-addr 710
lldp med-notification 711
lldp med-tlv inventory 712
lldp med-tlv location 713
lldp med-tlv med-cap 713
lldp med-tlv network-policy 714

- lldp notification 714
- lldp notification-interval 698
- lldp refresh-interval 699
- lldp reinit-delay 700
- lldp tx-delay 700
- location-led 112
- logging facility 145
- logging history 146
- logging host 147
- logging on 147
- logging sendmail 152
- logging sendmail destination-email 154
- logging sendmail host 152
- logging sendmail level 153
- logging sendmail source-email 154
- logging trap 148
- login 137

M

- mac access-group 362
- mac-address-table aging-time 443
- mac-address-table static 444
- mac-authentication intrusion-action 291
- mac-authentication max-mac-count 291
- mac-authentication reauth-time 283
- mac-learning 276
- mac-vlan 518
- management 264
- match 549
- match as-path 993
- match community 993
- match extcommunity 994
- match ip address 995
- match ip next-hop 995
- match ip route-source 996
- match metric 996
- match origin 997
- match pathlimit 997
- match peer 998
- max-current-dd 884
- max-hops 457
- maximum-paths 813
- maximum-prefix 825
- memory 198
- mst priority 458
- mst vlan 459
- mvr 635
- mvr associated-profile 635
- mvr domain 636
- mvr immediate-leave 642
- mvr profile 636
- mvr proxy-query-interval 637
- mvr proxy-switching 638
- mvr robustness-value 639
- mvr source-port-mode dynamic 640
- mvr type 643
- mvr upstream-source-ip 640
- mvr vlan 641

- mvr vlan group 644
- mvr6 associated-profile 654
- mvr6 domain 654
- mvr6 immediate-leave 661
- mvr6 profile 655
- mvr6 proxy-query-interval 656
- mvr6 proxy-switching 657
- mvr6 robustness-value 658
- mvr6 source-port-mode dynamic 659
- mvr6 type 662
- mvr6 upstream-source-ip 660
- mvr6 vlan 660
- mvr6 vlan group 663

N

- name 460
- negotiation 375
- neighbor 825
- neighbor activate 949
- neighbor advertisement-interval 950
- neighbor allowas-in 950
- neighbor attribute-unchanged 951
- neighbor capability dynamic 952
- neighbor capability orf prefix-list 952
- neighbor default-originate 953
- neighbor description 954
- neighbor distribute-list 954
- neighbor dont-capability-negotiate 955
- neighbor ebgp-multihop 956
- neighbor enforce-multihop 957
- neighbor filter-list 957
- neighbor interface 958
- neighbor maximum-prefix 959
- neighbor next-hop-self 960
- neighbor override-capability 960
- neighbor passive 961
- neighbor peer-group (Creating) 961
- neighbor peer-group (Group Members) 962
- neighbor port 963
- neighbor prefix-list 963
- neighbor remote-as 964
- neighbor remove-private-as 965
- neighbor route-map 966
- neighbor route-reflector-client 966
- neighbor route-server-client 967
- neighbor send-community 968
- neighbor shutdown 969
- neighbor soft-reconfiguration inbound 969
- neighbor strict-capability-match 970
- neighbor timers 971
- neighbor timers connect 972
- neighbor unsuppress-map 972
- neighbor update-source 973
- neighbor weight 974
- netbios-name-server 744
- netbios-node-type 745
- network 746
- network 826

Index of CLI Commands

network 938
network area 856
network-access aging 282
network-access dynamic-qos 284
network-access dynamic-vlan 285
network-access guest-vlan 286
network-access link-detection 286
network-access link-detection link-down 287
network-access link-detection link-up 287
network-access link-detection link-up-down 288
network-access mac-filter 282
network-access max-mac-count 288
network-access mode mac-authentication 289
network-access port-mac-filter 290
next-server 747
nlm 195
no rspan session 422
ntp authenticate 159
ntp authentication-key 160
ntp client 161
ntp server 161

O

on-match 999

P

parity 138
passive-interface 827
passive-interface 866
passive-interface 900
password 138
password-thresh 139
periodic 171
permit, deny 616
permit, deny (ARP ACL) 365
permit, deny (Extended IPv4 ACL) 350
permit, deny (Extended IPv6 ACL) 356
permit, deny (MAC ACL) 360
permit, deny (Standard IP ACL) 349
permit, deny (Standard IPv6 ACL) 355
pfc mode 570
pfc priority 571
ping 755
ping6 780
police flow 553
police srtcm-color 554
police trtcm-color 557
policy-map 551
port channel load-balance 402
port monitor 415
port security 277
pppoe intermediate-agent 267
pppoe intermediate-agent format-type 267
pppoe intermediate-agent port-enable 268
pppoe intermediate-agent port-format-type 269
pppoe intermediate-agent trust 270
pppoe intermediate-agent vendor-tag strip 270

private vlan association 509
private-vlan 508
process cpu 198
prompt 93
protocol-vlan protocol-group (Configuring Groups) 513
protocol-vlan protocol-group (Configuring Interfaces) 513

Q

qos map cos-dscp 534
qos map default-drop-precedence 535
qos map dscp-cos 536
qos map dscp-mutation 537
qos map ip-port-dscp 538
qos map ip-prec-dscp 539
qos map phb-queue 533
qos map trust-mode 540
queue mode 528
queue weight 529
quit 96

R

radius-server acct-port 222
radius-server auth-port 223
radius-server host 223
radius-server key 224
radius-server retransmit 225
radius-server timeout 225
range 617
rate-limit 426
rcommand 176
redistribute 827
redistribute 848
redistribute 889
redistribute 939
reload (Global Configuration) 94
reload (Privileged Exec) 98
rename 551
revision 460
rmon alarm 202
rmon collection history 204
rmon collection rmon1 205
rmon event 203
route-map 990
router bgp 921
router ipv6 ospf 882
router ospf 840
router pim 1020
router pim6 1043
router rip 822
router-id 843
router-id 885
rspan destination 420
rspan remote vlan 421
rspan source 419

S

server 234
service dhcp 738
service-policy 561
set aggregator as 999
set as-path 1000
set atomic-aggregate 1001
set comm-list delete 1001
set community 1002
set cos 559
set extcommunity 1003
set ip next-hop 1004
set local-preference 1005
set metric 1006
set origin 1006
set originator-id 1007
set pathlimit ttl 1008
set phb 560
set weight 1008
sflow 209
sflow destination 210
sflow max-datagram-size 211
sflow max-header-size 211
sflow owner 212
sflow polling-interval 212
sflow sample 213
sflow source 213
sflow timeout 214
show access-group 366
show access-list 367
show access-list tcam-utilization 112
show accounting 236
show arp 759
show arp access-list 366
show auto-traffic-control 441
show auto-traffic-control interface 442
show banner 111
show bridge-ext 481
show calendar 168
show class-map 561
show cluster 176
show cluster candidates 177
show cluster members 177
show cn 587
show cn cnpv 588
show cn cp 589
show dcbx 568
show dns 727
show dns cache 727
show dos-protection 341
show dot1q-tunnel 499
show dot1x 261
show ets mapping 578
show ets weight 579
show garp timer 482
show gvrp configuration 483
show history 96
show hosts 728
show interfaces brief 385
show interfaces counters 386
show interfaces history 390
show interfaces protocol-vlan protocol-group 515
show interfaces status 393
show interfaces switchport 394
show interfaces transceiver 396
show interfaces transceiver-threshold 397
show ip access-group 353
show ip access-list 353
show ip arp inspection configuration 337
show ip arp inspection interface 337
show ip arp inspection log 338
show ip arp inspection statistics 338
show ip arp inspection vlan 338
show ip bgp 974
show ip bgp attribute-info 976
show ip bgp cidr-only 976
show ip bgp community 977
show ip bgp community-info 978
show ip bgp community-list 978
show ip bgp dampening 979
show ip bgp filter-list 980
show ip bgp neighbors 981
show ip bgp paths 982
show ip bgp prefix-list 983
show ip bgp regexp 983
show ip bgp route-map 984
show ip bgp scan 984
show ip bgp summary 985
show ip community-list 985
show ip dhcp 748
show ip dhcp binding 748
show ip dhcp snooping 310
show ip dhcp snooping binding 311
show ip extcommunity-list 986
show ip helper 763
show ip host-route 813
show ip igmp filter 620
show ip igmp groups 678
show ip igmp interface 680
show ip igmp profile 621
show ip igmp query-drop 622
show ip igmp snooping 608
show ip igmp snooping group 609
show ip igmp snooping mrouter 1018
show ip igmp snooping mrouter 610
show ip igmp snooping statistics 611
show ip igmp throttle interface 622
show ip interface 752
show ip mroute 1012
show ip multicast-data-drop 623
show ip ospf 866
show ip ospf border-routers 868
show ip ospf database 869
show ip ospf interface 875
show ip ospf neighbor 877
show ip ospf route 878
show ip ospf virtual-links 878
show ip pim bsr-router 1040

Index of CLI Commands

show ip pim interface 1027
show ip pim neighbor 1028
show ip pim rp mapping 1041
show ip pim rp-hash 1042
show ip prefix-list 986
show ip prefix-list detail 987
show ip prefix-list summary 987
show ip protocols ospf 879
show ip protocols rip 837
show ip rip 838
show ip route 814
show ip route database 815
show ip route summary 816
show ip source-guard 323
show ip source-guard binding 324
show ip ssh 251
show ip telnet 243
show ip traffic 753
show ip traffic 816
show ipv6 access-group 358
show ipv6 access-list 357
show ipv6 dhcp relay destination 736
show ipv6 dhcp snooping 318
show ipv6 dhcp snooping binding 318
show ipv6 dhcp snooping statistics 319
show ipv6 interface 773
show ipv6 mld groups 690
show ipv6 mld interface 691
show ipv6 mld snooping 631
show ipv6 mld snooping group 632
show ipv6 mld snooping group source-list 632
show ipv6 mld snooping mrouter 633
show ipv6 mroute 1015
show ipv6 mtu 775
show ipv6 nd rguard 789
show ipv6 neighbors 790
show ipv6 ospf 900
show ipv6 ospf database 902
show ipv6 ospf interface 903
show ipv6 ospf neighbor 904
show ipv6 ospf route 905
show ipv6 ospf virtual-links 906
show ipv6 pim bsr-router 1063
show ipv6 pim interface 1050
show ipv6 pim neighbor 1051
show ipv6 pim rp mapping 1064
show ipv6 pim rp-hash 1064
show ipv6 route 819
show ipv6 source-guard 329
show ipv6 source-guard binding 329
show ipv6 traffic 775
show ipv6 tunnel 798
show l2protocol-tunnel 504
show lacp 410
show line 144
show lldp config 715
show lldp info local-device 716
show lldp info remote-device 717
show lldp info statistics 719
show location-led status 113
show log 149
show logging 150
show logging sendmail 155
show loop internal 398
show mac access-group 363
show mac access-list 363
show mac-address-table 445
show mac-address-table aging-time 446
show mac-address-table count 447
show mac-vlan 519
show management 265
show map default-drop-precedence 541
show map dscp-cos 542
show memory 113
show mvr 646
show mvr associated-profile 647
show mvr interface 647
show mvr members 648
show mvr profile 650
show mvr statistics 650
show mvr6 665
show mvr6 associated-profile 666
show mvr6 interface 666
show mvr6 members 667
show mvr6 profile 669
show mvr6 statistics 669
show network-access 292
show network-access mac-address-table 293
show network-access mac-filter 294
show nlm oper-status 197
show ntp 162
show pfc 572
show pfc statistics 573
show policy-map 562
show policy-map interface 563
show port monitor 416
show port security 279
show port-channel load-balance 413
show pppoe intermediate-agent info 271
show pppoe intermediate-agent statistics 272
show process cpu 114
show protocol-vlan protocol-group 514
show public-key 251
show qos map cos-dscp 541
show qos map dscp-mutation 543
show qos map ip-port-dscp 543
show qos map ip-prec-dscp 544
show qos map phb-queue 545
show qos map trust-mode 545
show queue mode 531
show queue weight 531
show radius-server 226
show reload 99
show rmon alarms 206
show rmon events 206
show rmon history 207
show rmon statistics 207
show route-map 1009

show rspan 422
 show running-config 114
 show sflow 214
 show snmp 183
 show snmp engine-id 192
 show snmp group 192
 show snmp notify-filter 197
 show snmp user 194
 show snmp view 194
 show snmp 158
 show spanning-tree 474
 show spanning-tree mst configuration 476
 show ssh 252
 show startup-config 116
 show subnet-vlan 517
 show system 116
 show tacacs-server 229
 show tech-support 118
 show time-range 172
 show traffic-segmentation 346
 show upgrade 133
 show users 118
 show version 119
 show vlan 492
 show vlan private-vlan 511
 show vlan-translation 506
 show voice vlan 525
 show vrrp 806
 show vrrp interface 808
 show vrrp interface counters 809
 show vrrp router counters 810
 show watchdog 120
 show web-auth 299
 show web-auth interface 299
 show web-auth summary 300
 shutdown 376
 silent-time 140
 snmp-server 181
 snmp-server community 181
 snmp-server contact 182
 snmp-server enable port-traps atc broadcast-alarm-clear 437
 snmp-server enable port-traps atc broadcast-alarm-fire 438
 snmp-server enable port-traps atc broadcast-control-apply 438
 snmp-server enable port-traps atc broadcast-control-release 439
 snmp-server enable port-traps atc multicast-alarm-clear 439
 snmp-server enable port-traps atc multicast-alarm-fire 440
 snmp-server enable port-traps atc multicast-control-apply 440
 snmp-server enable port-traps atc multicast-control-release 441
 snmp-server enable traps 184
 snmp-server engine-id 187
 snmp-server group 188
 snmp-server host 185
 snmp-server location 182
 snmp-server notify-filter 196
 snmp-server user 189
 snmp-server view 191
 snmp client 156
 snmp poll 157
 snmp server 158
 spanning-tree 450
 spanning-tree bpdu-filter 461
 spanning-tree bpdu-guard 462
 spanning-tree cost 463
 spanning-tree edge-port 464
 spanning-tree forward-time 451
 spanning-tree hello-time 452
 spanning-tree link-type 465
 spanning-tree loopback-detection 466
 spanning-tree loopback-detection action 466
 spanning-tree loopback-detection release 473
 spanning-tree loopback-detection release-mode 467
 spanning-tree loopback-detection trap 468
 spanning-tree max-age 452
 spanning-tree mode 453
 spanning-tree mst configuration 456
 spanning-tree mst cost 468
 spanning-tree mst port-priority 469
 spanning-tree pathcost method 454
 spanning-tree port-bpdu-flooding 470
 spanning-tree port-priority 471
 spanning-tree priority 455
 spanning-tree protocol-migration 473
 spanning-tree root-guard 471
 spanning-tree spanning-disabled 472
 spanning-tree system-bpdu-flooding 456
 spanning-tree transmission-limit 457
 speed 141
 stopbits 141
 subnet-vlan 516
 summary-address 850
 switchport acceptable-frame-types 487
 switchport allowed vlan 488
 switchport block 377
 switchport dot1q-tunnel mode 495
 switchport dot1q-tunnel service match cvid 496
 switchport dot1q-tunnel tpid 498
 switchport forbidden vlan 480
 switchport gvrp 480
 switchport ingress-filtering 489
 switchport l2protocol-tunnel 503
 switchport mode 489
 switchport mode private-vlan 509
 switchport mtu 378
 switchport native vlan 490
 switchport packet-rate 427
 switchport priority default 530
 switchport private-vlan host-association 510
 switchport private-vlan mapping 511
 switchport vlan-translation 504
 switchport voice vlan 523

Index of CLI Commands

switchport voice vlan priority 523
switchport voice vlan rule 524
switchport voice vlan security 525

T

tacacs-server host 227
tacacs-server key 227
tacacs-server port 228
tacacs-server retransmit 228
tacacs-server timeout 229
terminal 143
test loop internal 398
timeout login response 142
time-range 169
timers basic 829
timers bgp 940
timers spf 844
timers spf 886
traceroute 754
traceroute6 781
traffic-class algo 575
traffic-class map 576
traffic-class weight 577
traffic-segmentation 342
traffic-segmentation session 343
traffic-segmentation uplink/downlink 344
traffic-segmentation uplink-to-uplink 345
transceiver-monitor 379
transceiver-threshold current 380
transceiver-threshold rx-power 381
transceiver-threshold temperature 382
transceiver-threshold tx-power 383
transceiver-threshold voltage 384
transceiver-threshold-auto 379
tunnel destination 793
tunnel mode ipv6ip 795

tunnel source vlan 797
tunnel ttl 797

U

umount usbdisk 130
upgrade opcode auto 131
upgrade opcode path 132
upgrade opcode reload 133
username 219

V

version 830
vlan 485
vlan database 484
vlan-trunking 491
voice vlan 520
voice vlan aging 521
voice vlan mac-address 522
vrrp authentication 802
vrrp ip 802
vrrp preempt 803
vrrp priority 804
vrrp timers advertise 805

W

watchdog software 120
web-auth 297
web-auth login-attempts 295
web-auth quiet-period 296
web-auth re-authenticate (IP) 298
web-auth re-authenticate (Port) 298
web-auth session-timeout 296
web-auth system-auth-control 297
whichboot 130

Index

Numerics

- 802.1Q tunnel 493
 - access 495
 - configuration, guidelines 494
 - configuration, limitations 494
 - CVID to SVID map 496
 - ethernet type 498
 - interface configuration 495–498
 - mode selection 495
 - status, configuring 494
 - TPID 498
 - uplink 495
- 802.1X
 - authenticator, configuring 255–261
 - global settings 254–255
 - port authentication 253, 255
 - port authentication accounting 235

A

- AAA
 - accounting 802.1X port settings 235
 - accounting exec command privileges 231
 - accounting exec settings 235
 - accounting summary 236
 - accounting update 232
 - accounting, configuring 230
 - authorization & accounting 230
 - authorization exec settings 233, 236
 - authorization method 236
 - authorization settings 233
 - authorization summary 236
 - RADIUS group settings 234
 - TACACS+ group settings 234
- acceptable frame type 487
- Access Control List *See* ACL
- ACL 347
 - ARP 364
 - binding to a port 352
 - IPv4 Extended 347, 350
 - IPv4 Standard 347, 349
 - IPv6 Extended 354, 356
 - IPv6 Standard 354, 355
 - MAC 359
 - time range 169

- address table 443
 - aging time 443
 - aging time, displaying 446
 - aging time, setting 443
- administrative users, displaying 118
- ARP
 - ACL 332
 - configuration 756
 - inspection 330
 - proxy 758
 - statistics 753, 816
- ARP inspection
 - ACL filter 332
 - additional validation criteria 334
 - ARP ACL 364
 - enabling globally 331
 - enabling per VLAN 334
 - trusted ports 336
- ATC 428
 - control response 433
 - functional limitations 431
 - limiting traffic rates 430
 - shutting down a port 431
 - thresholds 434, 435
 - timers 431, 432
 - usage 430
- authentication
 - MAC address authentication 281, 289
 - MAC, configuring ports 281
 - network access 281, 289
 - public key 245
 - web 297
 - web authentication port information, displaying 299
 - web authentication, configuring ports 297
 - web authentication, re-authenticating address 298
 - web authentication, re-authenticating ports 298
 - web, configuring 297
- Automatic Traffic Control *See* ATC

B

- BGP
 - aggregate address 928
 - AS path access list 922
 - cluster ID 931
 - community list 923

Index

- confederation ID 932
- configuration guidelines 916
- description 907
- extended community list 925
- external BGP 908
- internal BGP 908
- IP prefix list 927
- message types 911
- multihop for eBGP neighbors 956
- neighbor configuration 949
- neighbor peer group 961, 962
- neighbor route map 966
- path attributes 909
- policy-based routing 988
- route map, configuring 990
- route map, neighbor 966
- route metrics 943
- route reflection 930
- route reflector client 966
- route reflectors 912
- route selection 943
- route server client 967
- route servers 916
- router ID 937
- BOOTP 750
- bootstrap router
 - PIM-SM 1030
 - PIMv6-SM 1054
- Border Gateway Protocol *See* BGP
- BPDUL
 - filter 461
 - flooding when STA disabled on VLAN 470
 - flooding when STA globally disabled 456
 - guard 462
 - ignoring superior BPDUs 471
 - selecting protocol based on message format 473
 - shut down port on receipt 462
- bridge extension capabilities, displaying 481
- broadcast packets, blocking 377
- broadcast storm, threshold 427

C

- class map
 - description 549
 - DiffServ 548
- CLI
 - command modes 86
 - showing commands 84
- clustering switches, management access 173
- CN
 - defense mode, global 585
 - defense mode, interface 587
 - dot1p priority map to CNPv 583
 - dot1p priority, alternate CNPv priority, global 584

- dot1p priority, alternate CNPv priority, interface 586
 - enabling
 - priority, congestion notification message 582
- command line interface *See* CLI
- committed burst size, QoS policy 553, 555, 557
- committed information rate, QoS policy 553, 554, 557
- community ports 506
- community string 65, 181
- community VLANs 508
- configuration file, DHCP download reference 73
- configuration files, restoring defaults 123
- configuration settings
 - restoring 68, 123, 125
 - saving 68, 123, 125
- congestion notification *See* CN
- console port, required connections 56
- CoS 540
 - configuring 527
 - default mapping to internal values 534
 - enabling 540
 - layer 3/4 priorities 532
 - priorities, mapping to internal values 534
 - queue mapping 533
 - queue mode 528
 - queue weights, assigning 529
- CoS/CFI to PHB/drop precedence 534
- CPU
 - status 114
 - utilization, setting trap 198
 - utilization, showing 114
- CVLAN to SPVLAN map 496

D

- Data Center Bridge Exchange *See* DCBX
- data center bridging 565
- Data Center Bridging *See* DCBX
- DCB exchange commands 565
- DCBX
 - enabling 566
 - message exchange mode 566
- default IPv4 gateway, configuration 752
- default IPv6 gateway, configuration 765
- default priority, ingress port 530
- designated router
 - PIM 1037
 - PIMv6 1060
- DHCP 750
 - address pool 738
 - class identifier 729
 - client 729, 750
 - client identifier 729
 - dynamic configuration 63
 - IPv4 relay service, enabling 734
 - relay service 733

- server 736
 - DHCP snooping 300
 - enabling 301
 - global configuration 301
 - information option 303
 - information option policy 304
 - information option, circuit ID 307
 - information option, enabling 303
 - information option, remote ID 303
 - information option, suboption format 303
 - policy selection 304
 - specifying trusted interfaces 308
 - trusted port 308
 - untrusted port 308
 - verifying MAC addresses 305
 - VLAN configuration 306
 - DHCPv6
 - IPv6 relay service, enabling 735
 - DHCPv6 snooping 311
 - enabling 312
 - global configuration 312
 - specifying trusted interfaces 315
 - trusted port 315
 - untrusted port 315
 - VLAN configuration 314
 - DiffServ 547
 - binding policy to interface 561
 - class map 548, 552
 - class map, description 549
 - classifying QoS traffic 549
 - color aware, srTCM 554
 - color aware, trTCM 557
 - color blind, srTCM 554
 - color blind, trTCM 557
 - committed burst size 553, 555, 557
 - committed information rate 553, 554, 557
 - configuring 547
 - conforming traffic, configuring response 553, 554, 557
 - description 549
 - excess burst size 555
 - metering, configuring 553
 - peak burst size 557
 - peak information rate 557
 - policy map 551
 - policy map, description 549
 - QoS policy 551
 - service policy 561
 - setting CoS for matching packets 559
 - setting PHB for matching packets 560
 - single-rate, three-color meter 554
 - srTCM metering 554
 - traffic between CIR and BE, configuring response 554
 - traffic between CIR and PIR, configuring response 557
 - trTCM metering 557
 - two-rate, three-color meter 557
 - violating traffic, configuring response 553, 554, 557
 - DNS
 - default domain name 723
 - displaying the cache 727
 - domain name list 724
 - enabling lookup 722
 - name server list 724
 - static entries, IPv4 724
 - static entries, IPv6 725
 - Domain Name Service *See* DNS
 - downloading software 125
 - automatically 131
 - using FTP or TFTP 125
 - DR priority, PIM-SM 1037
 - DR priority, PIMv6-SM 1060
 - drop precedence
 - CoS priority mapping 534
 - DSCP ingress map 537
 - DSA encryption 249
 - DSCP 540
 - enabling 540
 - mapping to internal values 537
 - DSCP ingress map, drop precedence 537
 - DSCP to PHB/drop precedence 537
 - dynamic addresses
 - clearing 445
 - displaying 445
 - Dynamic Host Configuration Protocol *See* DHCP
 - dynamic QoS assignment 284
 - dynamic VLAN assignment 285
- ## E
- ECMP, maximum paths 813
 - edge port, STA 464
 - encryption
 - DSA 249
 - RSA 249
 - engine ID 187
 - Enhanced Transmission Selection *See* ETS
 - ETS 575, 576
 - bandwidth allocation for TCGs 577
 - mode, negotiated or forced 574
 - event logging 145
 - excess burst size, QoS policy 555, 557
 - exec command privileges, accounting 231
 - exec settings
 - accounting 235
 - authorization 233, 236
 - external BGP 908

F

FIB, description 814
firmware
 displaying version 119
 upgrading 125
 upgrading automatically 131
 upgrading with FTP or TFTP 125
 version, displaying 119
forwarding information base See FIB

G

gateway, IPv4 default 752
gateway, IPv6 default 765
general security measures 275
GNU license 1071
GVRP
 enabling 478
 global setting 478
 interface configuration 480

H

hardware version, displaying 119
hash mask length, PIM-SM BSR 1030
hash mask length, PIMv6-SM BSR 1054
hello holdtime
 PIM 1022
 PIMv6 1045
hello interval
 PIM 1023
 PIMv6 1046
HTTP, web server 238
HTTPS 239
 configuring 239
 replacing SSL certificate 125
 secure-site certificate 125
 UDP port, configuring 239
HTTPS, secure server 239

I

IEEE 802.1D 453
IEEE 802.1s 453
IEEE 802.1w 453
IEEE 802.1X 253, 255
IGMP
 clearing groups 677
 enabling per interface 672
 filter profiles, binding to interface 617
 filter profiles, configuration 616
 filter, interface configuration 617–619
 filter, parameters 615–619
 filtering & throttling 614
 filtering & throttling, enabling 615

 filtering & throttling, interface configuration 617
 filtering & throttling, status 615
 filtering, configuring profile 616, 617
 filtering, creating profile 616
 filtering, group range 617
 filtering, interface settings 617–619
 groups, displaying 609
 interface configuration 672–677
 interface status, displaying 680
 last member query interval 673
 Layer 2 592
 Layer 3 671
 maximum response time 673
 multicast groups, displaying 678
 proxy 681
 proxy routing 681
 proxy routing, configuring 681
 proxy routing, interface configuration 671
 query 594
 query interval 674
 query, enabling 594
 report delay 673
 robustness value 675
 robustness variable 675
 showing groups 678
 snooping 592
 snooping & query, parameters 592
 snooping, configuring 592
 snooping, enabling 593
 snooping, immediate leave 601
 static groups, configuring 676
 version 677
IGMP proxy
 enabling 681
 unsolicited report interval 683
IGMP snooping
 configuring 592
 enabling per interface 593
 forwarding entries 609
 immediate leave, status 601
 interface attached to multicast router 610, 613
 last member query count 602
 last member query interval 603
 proxy query address 604
 proxy query interval 606
 proxy query response interval 606
 proxy reporting 594
 querier timeout 596
 querier, enabling 594
 router port expire time 596
 static host interface 607
 static multicast routing 613
 static port assignment 607
 static router interface 613

- static router port, configuring 613
- statistics, displaying 611
- TCN flood 596
- unregistered data flooding 598
- version exclusive 600
- version for interface, setting 599
- version, setting 599
- with proxy reporting 594
- immediate leave, IGMP snooping 601
- immediate leave, MLD snooping 630
- importing user public keys 125
- ingress filtering 489
- internal BGP 908
- IP address
 - BOOTP/DHCP 731
 - setting 749
- IP filter, for management access 264
- IP Port to PHB/drop precedence 538
- IP Precedence 540
 - enabling 540
- IP precedence to PHB/drop precedence 539
- IP routing 811
 - maximum paths 813
 - unicast protocols 811
- IP statistics 753, 775, 816
- IPv4 address
 - BOOTP/DHCP 750
 - dynamic configuration 63
 - manual configuration 60
 - setting 59, 750
- IPv4 source guard
 - configuring static entries 320
 - setting filter criteria 321
 - setting maximum bindings 323
- IPv6
 - configuring static neighbors 788
 - displaying neighbors 788, 790
 - duplicate address detection 783, 790
 - enabling 770
 - hop limit, router advertisements 783
 - MTU 772
 - neighbor solicitation interval 785
 - reachability time 787
 - relay desination 735
 - router advertisements, blocking 786
 - router advertisements, hop limit 783
- IPv6 address
 - dynamic configuration (link-local) 64, 770
 - EUI format 768
 - EUI-64 setting 767, 768
 - explicit configuration 770
 - global unicast 766
 - link-local 769
 - manual configuration (global unicast) 60, 766

- manual configuration (link-local) 60, 769
- setting 59, 766
- IPv6 source guard
 - configuring static entries 325
 - setting maximum bindings 328
- IPv6/v4 tunnel 791
 - IPv4 destination, configured 793
 - mode, configured or 6to4 795
 - source VLAN 797

J

- jumbo frame 122

K

- key
 - private 243
 - public 243
 - user public, importing 125
- key pair
 - host 243
 - host, generating 249

L

- LACP
 - admin key 406
 - configuration 401
 - group attributes, configuring 408
 - group members, configuring 404–407
 - local parameters 410
 - partner parameters 410
 - protocol message statistics 410
 - protocol parameters 401
 - timeout mode 409
 - timeout, for LACPDU 409
- last member query count, IGMP snooping 602
- last member query interval, IGMP snooping 603
- layer 2, protocol tunnel 503
- license information, GNU 1071
- Link Layer Discovery Protocol *See* LLDP
- link type, STA 465
- LLDP 695
 - device statistics details, displaying 719
 - device statistics, displaying 719
 - display device information 717
 - displaying remote information 717
 - ETS advertised settings 705
 - ETS, advertised PFC configuration 706
 - interface attributes, configuring 701–714
 - local device information, displaying 716
 - message attributes 695
 - message statistics 719
 - remote information, displaying 717

- remote port information, displaying 717
- timing attributes, configuring 697–700
- TLV, 802.1 706–708
- TLV, 802.3 708–709
- TLV, basic 701–704
- TLV, ETS 704–706
- TLV, ETS configuration 704
- TLV, management address 701
- TLV, port description 702
- TLV, system capabilities 703
- TLV, system description 703
- TLV, system name 704
- LLDP-MED 695
 - end-node, extended power-via-MDI 718
 - end-node, inventory 718
 - end-node, location 718
 - end-node, network policy 718
 - notification, status 711
 - TLV 695
 - TLV, inventory 712
 - TLV, location 710, 713
 - TLV, MED capabilities 713
 - TLV, network policy 714
- local engine ID 187
- logging
 - messages, displaying 149
 - syslog traps 148
 - to syslog servers 147
- logon authentication 217
 - encryption keys 224, 227
 - RADIUS client 222
 - RADIUS server 222
 - sequence 220, 221
 - settings 221
 - TACACS+ client 226
 - TACACS+ server 226
- logon authentication, settings 222, 226
- logon banner, configuring 102
- loopback detection, STA 466
- loopback test, port 398

M

- MAC address authentication 281
 - ports, configuring 281, 289
 - reauthentication 283
- MAC address, mirroring 415
- management access, filtering per address 264
- management access, IP filter 264
- matching class settings, classifying QoS traffic 549
- memory
 - status 113
 - utilization, showing 113
- memory utilization, setting trap 198
- mirror port
 - configuring local traffic 415
 - configuring remote traffic 417
- mirror port, configuring 415
- MLD
 - cache, clearing 689
 - enabling on VLAN 684
 - groups, displaying 690
 - last member query response interval 684
 - maximum response interval 685
 - proxy routing
 - proxy routing, enabling 692
 - query interval 686
 - robustness value 687
 - static groups, binding 687
 - version 688
- MLD snooping 624
 - configuring 624
 - enabling 625
 - immediate leave 630
 - immediate leave, status 630
 - multicast static router port 629
 - querier 625
 - querier, enabling 625
 - query interval 626
 - query, maximum response time 626
 - robustness value 627
 - static port assignment 630
 - static router port 629
 - unknown multicast, handling 628
 - version 629
- MSTP 453
 - global settings, configuring 449
 - global settings, displaying 474
 - interface settings, configuring 450
 - interface settings, displaying 474
 - max hop count 457
 - path cost 468
 - region name 460
 - region revision 460
- MTU for IPv6 772
- multicast filtering 591
 - enabling IGMP snooping 593
 - enabling IGMP snooping per interface 593
 - enabling MLD snooping 625
 - router configuration 613
- multicast groups 609
 - static 607, 609
- Multicast Listener Discovery *See* MLD
- Multicast Listener Discovery *See* MLD snooping
- multicast router discovery 603
- multicast router port, displaying 610
- multicast routing 1011
 - ECMP 813

- ECMP maximum paths 813
- enabling, IPv4 1011
- enabling, IPv6 1014
- global settings, IPv4 1011
- global settings, IPv6 1014
- PIM 1019
- PIM-DM 1019
- PIM-SM 1019
- PIMv6 1042
- PIMv6-SM 1054
- reverse path tree 1039, 1062
- routing table, IPv4 1012
- routing table, IPv6 1015
- upstream interface 1014, 1016
- multicast services
 - configuring 607
 - displaying 609
- multicast static router port 613
 - configuring 613
 - configuring for MLD snooping 629
- multicast storm, threshold 427
- multicast, filtering and throttling 615
- multicast, static router port 1017
- MVR
 - assigning static multicast groups 636, 644
 - configuring 633, 641
 - interface status, configuring 642–644
 - interface status, displaying 646
 - IP for control packets sent upstream 640
 - proxy query interval 637
 - proxy switching 638
 - receiver groups, displaying 648
 - robust value for proxy switching 639
 - setting interface type 643
 - setting multicast domain 636
 - setting multicast groups 635, 636
 - source port mode 640
 - specifying a domain 636
 - specifying a VLAN 635, 641
 - static binding 636, 644
 - static binding, group to port 644
 - statistics, displaying 650
 - using immediate leave 642
- MVR6
 - assigning static multicast groups 655, 663
 - configuring 653, 660
 - interface status, configuring 661–663
 - interface status, displaying 667
 - IP for control packets sent upstream 660
 - proxy query interval 637
 - proxy switching 657
 - receiver groups, displaying 667
 - robust value for proxy switching 658
 - setting interface type 662

- setting multicast domain 654
- setting multicast groups 655
- source port mode 640
- specifying a domain 654
- specifying a VLAN 660
- static binding 655, 663
- static binding, group to port 663
- statistics, displaying 669
- using immediate leave 661

N

- network access
 - authentication 281
 - dynamic QoS assignment 284
 - dynamic VLAN assignment 285
 - guest VLAN 286
 - MAC address filter 282
 - port configuration 289
 - reauthentication 283
 - secure MAC information 293, 294

NTP

- authentication keys, specifying 160
- setting the system clock 161–162
- specifying servers 161

O

- Open Shortest Path First *See* OSPF
- Open Shortest Path First (Version 3) *See* OSPFv3
- OSPF 839
 - ABR route summary 846
 - ABR/ASBR routing table, displaying 868
 - area border router 846
 - AS summary route 850
 - authentication key 859
 - authentication type 857
 - auto cost for an interface 847
 - autonomous system boundary router 842
 - backbone 857
 - configuration settings, displaying 866
 - cost for interface 860
 - default cost for summary route 845
 - default external route 842
 - default metric for external routes 848
 - enabling 840
 - general settings 839
 - hello interval 861
 - interface summary information, displaying 875
 - LSA advertisement interval 864
 - LSA database, displaying 869
 - message digest key 862
 - neighboring router information, displaying 877
 - network area 856
 - normal area 856

- NSSA 851
- process ID 840
- process parameters, displaying 879
- redistributing external routes 848
- retransmit interval 864
- RFC 1583 compatible 841
- route summary, ABR 846
- router ID 843
- router priority 863
- routing table, displaying 878
- SPF timers 844
- stub 852
- transit area 854
- transmit delay over interface 865
- virtual link 854
- virtual links, displaying 878

OSPFv3 880

- ABR route summary 887
- area border router 887
- backbone 893, 894
- configuration settings, displaying 900
- enabling 882
- general settings 880
- interface summary information, displaying 903
- LSA database, displaying 902
- neighboring router information, displaying 904
- network area 893
- normal area 893, 894
- process ID 882
- redistributing external routes 889
- route summary, ABR 887
- router ID 885
- routing table, displaying 905
- SPF timers 886
- stub 890
- transit area 891
- virtual link 891
- virtual links, displaying 906

P

packet block

- broadcast 377
- multicast 377
- unknown multicast 377
- unknown unicast 377

password, line 138

passwords 57, 218

- administrator setting 219

path cost 463

- method 454
- STA 454, 463

peak burst size, QoS policy 557

peak information rate, QoS policy 557

per-hop behavior, DSCP ingress map 537

PFC

- mode of operation 570
- priorities, enabling 571

PHB/drop precedence to CoS/CFI 536

PIM 1019

- configuring 1019
- dense-mode attributes 1019, 1028
- designated router 1037
- enabling for interfaces 1021
- enabling globally 1020
- hello holdtime 1022
- hello interval 1023
- interface settings 1021–1038
- neighbor routers, displaying 1028
- sparse-mode attributes 1020, 1030

PIM-DM 1019

- configuring 1019
- global configuration 1020
- interface settings 1021–1028
- neighbor routers 1028

PIM-SM 1019

- bootstrap router 1030
- BSR candidate 1030
- BSR elected, displaying 1040, 1063
- configuring 1019
- DR priority 1037
- global configuration 1020
- hash mask length for BSR 1030
- interface settings 1021–1028
- neighbor routers 1028
- register rate limit for DR 1032
- rendezvous point 1033, 1035
- RP candidate 1035
- RP candidate, advertising 1035
- RP mapping, displaying 1041, 1064
- shared tree 1013, 1016, 1037
- shortest path tree 1013, 1016, 1036
- SPT threshold 1036
- static RP, configuring 1033

PIMv6 1042

- configuring 1042
- dense mode, enabling 1044
- dense-mode attributes 1043, 1051
- designated router 1060
- enabling for interfaces 1044
- enabling globally 1043
- global configuration 1043
- graft retry interval 1051
- hello holdtime 1045
- hello interval 1046
- interface settings 1044–1049, 1060–1061
- max graft retries 1052
- neighbor routers 1051
- neighbor routers, displaying 1051

- prune delay 1047
- prune state, hold time 1046
- sparse-mode attributes 1043, 1054
- state refresh message interval 1053
- triggered hello delay 1049
- PIMv6-DM
 - global configuration 1020
 - interface settings 1051
- PIMv6-SM 1054
 - bootstrap router 1054
 - BSR candidate 1054
 - BSR elected, displaying 1063
 - configuring 1054
 - DR priority 1060
 - global configuration 1054–1059
 - hash mask length for BSR 1054
 - interface settings 1060
 - register rate limit for DR 1055
 - rendezvous point 1056, 1058
 - RP candidate 1058
 - RP candidate, advertising 1058
 - RP mapping, displaying 1064
 - shared tree 1060
 - shortest path tree 1059
 - SPT threshold 1059
 - static RP, configuring 1056
- policy map
 - description 549
 - DiffServ 551
- port authentication 253, 255
- port priority
 - configuring 527
 - default ingress 530
 - STA 469, 471
- port security, configuring 276
- ports
 - autonegotiation 375
 - broadcast storm threshold 427
 - capabilities 372
 - configuring 369
 - flow control 373
 - loopback test 398
 - mirroring 415
 - mirroring local traffic 415
 - mirroring remote traffic 417
 - mtu 378
 - multicast storm threshold 427
 - statistics 386
 - unknown unicast storm threshold 427
- PPPoE 266–272
- primary VLAN 508
- priority map to traffic class group 576
- priority, default port ingress 530
- priority-based flow control *See* PFC

- private key 243
- private VLANs, configuring 506
- private VLANs, displaying 511
- problems, troubleshooting 1069
- promiscuous ports 506
- protocol migration 473
- protocol tunnel, layer 2 503
- protocol VLANs 512
 - configuring 512
 - configuring groups 513
 - configuring interfaces 513
 - group configuration 513
 - interface configuration 513
- proxy ARP 758
- proxy query address, IGMP snooping 604
- proxy query interval, IGMP snooping 606
- proxy query response interval, IGMP snooping 606
- proxy reporting, IGMP snooping 594
- public key 243
- PVID, port native VLAN 490
- PVLAN
 - association 509
 - community ports 506
 - configuring 506
 - displaying 511
 - interface configuration 509, 510
 - primary VLAN 508
 - promiscuous ports 506

Q

- QoS 547
 - configuration guidelines 548
 - configuring 547
 - CoS/CFI to PHB/drop precedence 534
 - DSCP to PHB/drop precedence 537
 - dynamic assignment 284
 - IP Port to PHB/drop precedence 538
 - IP precedence to PHB/drop precedence 539
 - matching class settings 549
 - PHB to drop precedence, for untagged packets 535
 - PHB to queue 533
 - PHB/drop precedence to CoS/CFI 536
 - selecting CoS, DSCP, IP Precedence 540
- QoS policy
 - committed burst size 553, 555, 557
 - excess burst size 555
 - peak burst size 557
 - srTCM 554
 - srTCM police meter 554
 - trTCM 557
 - trTCM police meter 557
- QoS policy, committed information rate 553, 554, 557
- QoS policy, peak information rate 557
- queue mode, setting 528

queue weight, assigning to CoS 529

R

RADIUS

- logon authentication 222
- settings 222

rate limit

- port 426
- setting 425

register rate limit, PIM-SM 1032

register rate limit, PIMv6-SM 1055

remote engine ID 187

remote logging 148

Remote Monitoring *See* RMON

rename, DiffServ 551

rendezvous point

- PIM-SM 1033, 1035
- PIMv6-SM 1056, 1058

restarting the system 94, 98, 99

- at scheduled times 94

RIP

- authentication key 832
- authentication mode 831
- clearing routes 836
- configuration settings, displaying 838
- configuring 822–838
- default external route 822
- default metric 823
- global settings 822–829
- interface protocol settings 826–836
- interface, enabling 826
- neighbor router 825
- passively monitoring updates 827
- poison reverse 836
- process parameters, displaying 837
- protocol packets, receiving 833
- protocol packets, sending 835
- receive version 832
- redistributing external routing information 827
- routes, clearing 836
- routes, displaying 838
- routing table, clearing 836
- send version 834
- specifying interfaces 826
- split horizon 836
- timers 829
- version 830

RMON

- alarm, displaying settings 206
- alarm, setting thresholds 202
- commands 201
- event settings, displaying 206
- response to alarm setting 203
- statistics history, collection 204

- statistics history, displaying 207

- statistics, collection 205

- statistics, displaying 207

root guard 471

router redundancy

- protocols 801
- VRRP 801

Routing Information Protocol *See* RIP

routing information base, description 815

routing table, displaying 813, 814

RSA encryption 249

RSTP

- global settings, configuring 453
- global settings, displaying 474
- interface settings, configuring 461–472
- interface settings, displaying 474

running configuration files, displaying 114

S

scheduling algorithm 575

secure shell 243

- configuration 244

security, general measures 275

serial port, configuring 134

sFlow

- flow configuration 209–214
- target device 210

shared tree

- PIM-SM 1013, 1016, 1037
- PIMv6-SM 1060

shortest path tree

- PIM-SM 1013, 1016, 1036
- PIMv6-SM 1059

SMTP

- event handling 152
- sending log events 152

SNMP

- community string 181
- enabling traps 184
- filtering IP addresses 264
- global settings, configuring 181
- trap manager 185

SNMPv3

- 187–189
- engine ID 187
- engine identifier, local 187
- engine identifier, remote 187
- groups 188
- local users, configuring 189
- remote users, configuring 189
- user configuration 189
- views 191

SNTP

- setting the system clock 156–158
- specifying servers 158

- software
 - displaying version 119
 - downloading 125
 - version, displaying 119
 - SPT threshold, PIM-SM 1036
 - SPT threshold, PIMv6-SM 1059
 - srTCM
 - police meter 554
 - QoS policy 554
 - SSH 243
 - authentication retries 246
 - configuring 244
 - downloading public keys for clients 125
 - generating host key pair 249
 - server, configuring 246
 - timeout 248
 - STA 449
 - BPDU filter 461
 - BPDU flooding 470
 - BPDU shutdown 462
 - detecting loopbacks 466
 - edge port 464
 - forward delay 451
 - global settings, configuring 450–457
 - global settings, displaying 474
 - hello time 452
 - interface settings, configuring 461–472
 - interface settings, displaying 474
 - link type 465
 - loopback detection 466
 - maximum age 452
 - MSTP interface settings, configuring 468, 469
 - MSTP path cost 468
 - path cost 454, 463
 - path cost method 454
 - port priority 469, 471
 - port/trunk loopback detection 466
 - protocol migration 473
 - transmission limit 457
 - startup files
 - creating 125
 - displaying 116, 130
 - setting 124
 - static addresses, setting 444
 - static routes, configuring 812
 - statistics
 - ARP 753, 816
 - history for port 390
 - history for trunk 390
 - ICMP 753, 816
 - IP 753, 816
 - port 386
 - TCP 753, 816
 - UDP 753, 816
 - VLAN 386
 - STP 453
 - Also see* STA
 - summary, accounting 236
 - summer time, setting 163–165
 - switch clustering, for management 172
 - switch settings
 - restoring 123
 - saving 123
 - system clock
 - setting 155
 - setting manually 167
 - setting the time zone 167
 - setting with NTP 161–162
 - setting with SNTP 156–158
 - summer time 163–165
 - system logs 147
 - system software, downloading from server 125
- ## T
- TACACS+
 - logon authentication 226
 - settings 226
 - TCN
 - flood 596
 - general query solicitation 597
 - Telnet
 - configuring 241
 - server, enabling 242
 - telnet connection, configuring 134
 - terminal, configuration settings 143
 - time range, ACL 169
 - time zone, setting 167
 - time, setting 155
 - TPID 498
 - traffic segmentation 342
 - assigning ports 342, 343, 344
 - enabling 342, 343
 - sessions, assigning ports 342, 343, 344
 - sessions, creating 342, 343
 - trap manager 66, 185
 - troubleshooting 1069
 - trTCM
 - police meter 557
 - QoS policy 557
 - trunk
 - configuration 401
 - LACP 401, 404
 - load balancing 402
 - static 404
 - tunneling unknown VLANs, VLAN trunking 491

U

- UDP helper 760
 - application port 760
 - application server 762
 - destination port 760
 - enabling 761
 - forward destination 762
 - target subnet 762
 - UDP ports 760
- unicast routing 811
- unknown multicast packets, blocking 377
- unknown unicast packets, blocking 377
- unknown unicast storm, threshold 427
- unregistered data flooding, IGMP snooping 598
- upgrading software 125, 131
- upstream interface, multicast route 1014, 1016
- user account 218, 219
- user password 218, 219

V

- VLAN trunking 491
- VLANs 477–525
 - 802.1Q tunnel mode 495
 - acceptable frame type 487
 - adding static members 488
 - basic information, displaying 481
 - configuring port members, by interface 487–490
 - creating 485
 - displaying port members 492
 - dynamic assignment 285
 - egress mode 489
 - ingress filtering 489
 - interface configuration 487–491
 - IP subnet-based 516
 - MAC-based 518
 - mirroring 415
 - port members, displaying 492
 - private 506
 - protocol 512

- protocol, configuring 512
- protocol, configuring groups 513
- protocol, configuring interfaces 513
- protocol, group configuration 513
- protocol, interface configuration 513
- PVID 490
- statistics 386
- tag swapping 504
- translation, customer and service provider 504
- tunneling unknown groups 491
- voice 519
- voice VLANs 519
 - detecting VoIP devices 520
 - enabling for ports 523–525
 - identifying client devices 522
- VoIP traffic 519
 - ports, configuring 523–525
 - telephony OUI, configuring 522
 - voice VLAN, configuring 519
- VoIP, detecting devices 524
- VRRP 801
 - authentication 802
 - configuration settings 801
 - group statistics 806
 - preemption 803
 - priority 804
 - protocol message statistics 810
 - timers 805
 - virtual address 802

W

- web authentication 297
 - address, re-authenticating 298
 - configuring 297
 - configuring ports 297
 - port information, displaying 299
 - ports, configuring 297
 - ports, re-authenticating 298

